情報セキュリティ監査制度利用促進等事業　実施報告書

第１編　技術部会

平成 17 年 3 月 31 日

特定非営利活動法人　日本セキュリティ監査協会

まえがき

特定非営利活動法人日本セキュリティ監査協会における、「社会に貢献できる公正かつ公平な情報セキュリティ監査の普及・浸透」を目的とする諸活動の中にあって、技術部会は、とりわけ情報セキュリティ監査技術の向上を目的として、監査マニュアルの作成、監査手法の調査研究、監査ノウハウの蓄積を通して、有効かつ効率的な監査を提供するための基盤作りを行うことをその役割としている。すなわち監査アプローチ、監査技術、監査基盤の各領域の調査研究を対象としている。

これら３領域の調査研究のため、技術部会は３つのワーキンググループを発足し、活動してきた。

第１のワーキンググループは、監査アプローチを対象領域とし、昨年度は「情報セキュリティ監査助言方監査マニュアル」を取りまとめた。今年度は、将来的に「保証型監査マニュアル」策定を目標とし、そのフェイズ１として保証型監査等の諸監査概念の比較・検討を行っている。

第２のワーキンググループは、監査手法を対象領域とし、昨年度は「技術的検証項目」の調査研究に着手し、今年度は、「ＩＤＣサービス」をモデルとし、当該モデル環境における詳細な技術的情報セキュリティ管理基準の策定を行った。

第３のワーキンググループは、監査基盤を対象領域とし、昨年度は、「リスクアセスメントの調査報告書」を公表した。今年度は、リスクアセスメント手法の適用方法および個別情報資産に関連する脅威-脆弱性の研究を行った。

それぞれの報告は、技術部会構成員により日常業務で多忙な中、その寸暇を惜しんで取りまとめられたものである。執筆・査閲の労をとられた方々に、ここに改めて感謝の意を表したい。

情報セキュリティは、国家プロジェクトであるｅ－Ｊａｐａｎ戦略の重要なファクタとして位置付けられている。技術部会構成員の英知の結晶である本報告が、その一端を担っていれば幸いである。

平成17年3月31日

日本セキュリティ監査協会
技術部会長　和貝享介

第１編　第１部　技術部会ＷＧ１

情報セキュリティ監査および周辺領域についての
中間報告書

平成 17 年 3 月 31 日

第１編　第１部　目次

１．中間報告書の目的 8
２．保証型監査、合意された手続、助言型監査、コンサルティングの異同 9
　２．１　保証型監査 10
　２．２　合意された手続 15
　２．３　助言型監査 18
　２．４　コンサルティング 19
　２．５　今後整理すべき業務形態 21
３．情報セキュリティ監査、システム監査、ISMS 審査の異同 22
　３．１　情報セキュリティ監査 25
　３．２　システム監査 28
　３．３　ISMS 適合性評価制度 30
参考文献 33

１．中間報告書の目的

情報セキュリティ監査は大別すると助言型監査と保証型監査がある。助言型監査、保証型監査の考え方は、情報セキュリティ監査制度で導入された考え方であり、その概念を一般に浸透させるためには、更に、詳細な検討が必要である。助言型監査は、従来から行われていたシステム監査の考え方を取り入れたものであり、保証型監査は、会計監査の考え方を取り入れたものである。また、情報セキュリティ監査に関連する ISMS 審査やシステム監査も行われており、これらと情報セキュリティ監査の相違も明確にすることが、情報セキュリティ監査の普及に不可欠である。

2003 年度の研究では助言型監査マニュアルの策定を行った。次に必要とされるのは保証型監査マニュアルであるが、上記の点を考慮すると、保証型監査マニュアルの検討に入る前に、情報セキュリティ監査の概念についてより詳細に定義をすることが望ましい。

このため、2004 年度は情報セキュリティ監査を、類似の行為や関連する諸制度と比較し、その概念をより詳細にすることを目的とした。また、監査の分類として内部監査と外部監査の分別もあるが、本報告書は外部監査を対象とする。

２．保証型監査、合意された手続、助言型監査、コンサルティングの異同

本章では、保証型監査、助言型監査といった監査意見の違いについての異同を検討する。情報セキュリティ監査制度では、報告基準ガイドラインにおいて、上記２つの監査以外に合意された手続が紹介されている。また、助言型監査と一般のコンサルティングとの違いが不明確という話もある。このため本章では、保証型監査、合意された手続、助言型監査、コンサルティングの異同を説明することにする。各々の詳細は後述するが、これら異同点を要約すると下記のとおりとなる。

表 1　保証型監査、合意された手続、コンサルティングの比較

	保証型監査	合意された手続	助言型監査	コンサルティング
保証	与える	与えない 実施した項目の適否のみを言明する	与えない	与えない
意見	述べる	述べない	述べる	述べる
提言	しない	しない	する	する
客観的基準	存在することが前提	利害関係者で合意された手続が必要	存在することが前提	ない
実施者の独立性	必須	必須	必須	必須ではない
監査結果報告先	経営者若しくはそれに該当する役職者	経営者若しくはそれに該当する役職者	経営者若しくはそれに該当する役職者	依頼部門の長若しくは、それに該当する役職者
提言のフォローアップ	なし	なし	あり	なし

監査（保証型監査と助言型監査）は客観的基準を元に判断する点が他と異なる。また、

監査人の独立性が必須であることが、コンサルティングと異なっている。

保証型監査と助言型監査の基本的相違点は、保証を与えるか否かである。いうまでもなく、前者は保証を与え、後者は助言にとどまる。

合意された手続は、保証を与えず合意された手続をした結果のみを報告する。監査人の独立性は必須となる。ただし、他のものと相違し、監査意見は述べない。また、依頼者と監査主体または被監査主体との間で合意された手続の存在が必須である。

保証型監査、合意された手続、助言型監査とコンサルティングの異動は、前者が監査対象者、利害関係者（想定利用者)、監査人という三者間の関係が必要であるのに対し、後者はコンサルティング先とコンサルタントの二者間の関係である点である。また、コンサルティングは 2 者関係のため独立性の問題は生じ得ない。また、基準は顧客との合意によるものであり、客観的である必要はない。しかし、コンサルタントの専門性に基づき、意見を述べることが求められる。

２．１　保証型監査

保証型監査とは、対象事象についての客観的な規準が存在することを前提として、入手した十分かつ適切な証拠に基づきその基準への準拠性について対象事象を評価又は測定し、その結果について独立の第三者として意見又は結論を表明することにより、対象事象に対して一定の信頼性を付与するものをいう。

情報セキュリティ監査における保証型監査とは、監査対象たる情報セキュリティのマネジメント又はコントロールが、監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を監査意見として表明する形態の監査をいう。

上記定義を行うにあたり参考としたものは、以下の通りである。

情報セキュリティ監査基準　実施基準ガイドライン

2.1　（前略）情報セキュリティ監査には、組織体が採用している情報セキュリティ対策の適切性に対して一定の保証を付与することを目的とする監査（保証型の監査という）と、（後略）

2.3　保証型の監査とは、監査対象たる情報セキュリティのマネジメント又はコントロールが、監査手続を実施した限りにおいて適切である旨（又は不適切である旨）を監査意見として表明する形態の監査をいう。（後略）

保証業務フレームワーク検討ＰＴ報告書

公認会計士が行う保証業務に関するフレームワーク（試案）

平成 16 年 7 月 6 日

日本公認会計士協会

【1 ページ】

公認会計士等が行う保証業務とは、業務対象についての客観的な作成又は実施の基準又は規準（以下「基準」という。）が存在することを前提として、入手した十分かつ適切な証拠に基づきその基準への準拠性について業務対象を評価又は測定（以下「評価」という。）し、その評価結果について独立の第三者として意見又は結論（以下「意見」という。）を表明することにより、業務対象に対して一定の信頼性を付与するものをいう。

企業会計審議会

財務情報等に係る保証業務の概念的枠組みに関する意見書

平成 16 年 11 月 29 日

企業会計審議会

【4 ページ】

1　保証業務の定義

保証業務とは、主題に責任を負う者が一定の規準によって当該主題を評価又は測定した結果を表明する情報について、又は、当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入手した証拠に基づき規準に照らして判断した結果を結論として報告する業務をいう。

JIS Q 19011:2003 品質及び／又は環境マネジメントシステム監査のための指針

監査の定義

3.1 監査

所定の監査基準*が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための体系的で、独立し、文書化されたプロセス。

*：監査基準は、Criteria すなわち、監査の判断尺度のことを意味している。

２．１．１　保証型監査の成立要件

保証型監査が成立するためには、少なくとも次の５つの要素が存在しそれぞれの要素に関する要件に適格である必要がある。

1. 監査人、監査対象について責任を負う者、利害関係者（想定利用者）の三当事者の存在
2. 適切な監査対象
3. 客観的な規準（適合する規準）
4. 十分かつ適切な監査証拠
5. 保証報告書

２．１．２　規準の要件

保証型監査には、監査目的を達成するために適合する客観的な規準の存在が必要である。情報セキュリティ監査の場合は、情報セキュリティ管理規準が想定されているが、それ以外の規準を用いることもできる。それ以外の規準を用いる場合は、企業会計審議会の「財務情報等に係る保証業務の概念的枠組みに関する意見書」を参考として規準を用いることが有益である。

（1）目的適合性

想定利用者による意思決定に役立つ結論を導くのに資する規準であること

（2）完全性

各業務環境の下で得られる結論に影響を与える要因のうち関連する要因のいずれもが省略されていない規準であること。なお、目的適合的であるならば、表示及び開示の規準が含まれる。

（3）信頼性

同一の環境で同一の資格を有する業務実施者が利用するとき、主題の評価又は測定を合理的にかつ首尾一貫して行うことができる信頼性のある規準であること

（4）中立性

偏向のない結論を導くのに資する中立的な規準であること

（5）理解可能性

明瞭かつ総合的な結論を導くことに資するもので、著しく異なる解釈をもたらすことなく、保証業務を構成する三当事者にとって理解可能な規準であること

２．１．３　課題

最後に保証型監査を行うにあたっての課題を指摘しておく。

■　意思決定の適正性の評価と準拠性の評価

保証型監査をする場合には、評価し、保証する範囲はどこまでか、ということが問題となる。評価し、保証する範囲の違いにより次の２つの監査がありうる。

①　意思決定の適正性の評価を行うか

つまり、リスクに応じた適切なコントロールが整備・運用されていることを評価するのか

②　意思決定の適正性の評価は行わず、決められたことを行っていることの評価を行うのか

つまり、決められたコントロールが運用されていることを評価するのか

これら２つの監査は、同じ保証型監査であっても、保証していることが異なるため、同じ保証型監査という名称でよいのか、報告書の文言は同じでよいのか、等を検討する必要がある。

■ 保証水準

保証型監査において、どの程度の心証を得るのかにより保証水準が異なってくる。公認会計士が行う、Trust サービスなどの保証業務のように合理的保証業務（高水準の保証）をするのか、限定的保証業務（中水準の保証。公認会計士の世界ではレビューと呼ばれている）をするのか、両方をするのか。両方をする場合は、その違いをどのように報告書上で表現すべきかを今後決める必要がある。

２．２　合意された手続

合意された手続の定義

合意された手続とは、対象を評価又は測定するために依頼者との間で合意された手続が存在することを前提として、実施した手続の結果について独立の第三者として結論を表明することをいう。

情報セキュリティ監査基準　報告基準ガイドライン

3.1　外部の情報セキュリティ監査人による監査では、選択適用すべき検証手続を監査依頼者と協議の上で決定し、それに対する結論のみを報告する契約を締結できる。

3.2　監査依頼者と合意した監査手続を実施し、その結論のみを報告する契約による場合、情報セキュリティ監査人と監査依頼者は、作成される報告書は情報セキュリティ対策の適否について保証を付与するものではないことに合意することができる。

保証業務フレームワーク検討ＰＴ報告書

公認会計士が行う保証業務に関するフレームワーク（試案）

平成 16 年 7 月 6 日

日本公認会計士協会

【P33】

合意された手続の目的は、公認会計士等が業務依頼者との間で合意した手続を実施し、その実施結果を報告することである。

公認会計士等の報告は、合意された手続の実施結果の事実に関してのみ行われ、いかなる意見も表明しない。

したがって、利用者は公認会計士等から報告された手続及び実施結果に基づき、自らの責任で結論を導くことが予定されている。

実施結果報告書は、実施すべき手続を合意した関係者のみにその配布が限定される。それは、これらの手続が採用された背景を知らない者は、実施結果について誤った理解をす

る可能性があるからである。

なお、合意された手続と保証型監査とならない点については、企業会計審議会の「財務情報等に係る保証業務の概念的枠組みに関する意見書」の以下の説明が参考となる。

① 業務実施者が、主題に責任を負う者又は特定の利用者との間で合意された手続に基づき発見した事項のみを報告する業務（「合意された手続」という。）。これは、実施される手続が主題に責任を負う者又は限られた利用者との間の合意によって特定されるため、業務実施者が自らの判断により証拠を入手しないこと、及び、手続の結果のみが報告され結論が報告されないことから、保証業務の定義を満たさない。

２．２．１　例示

合意された手続の例示を示すと次の通りとなる。

7.2.3 パスワードの割当ては、正規の管理手続によって統制すること			
管理基準　サブコントロール		合意された手続	実施した結果
7.2.3.1	パスワード管理手続の取組において、個人のパスワードを秘密に保つこと	情報セキュリティ関連規程等を査閲し、個人のパスワードを秘密に保つことがルール化されていることを確認する。	パスワード管理規則を査閲し、個人のパスワードを秘密に保つことが規定されていたことを確認した。
7.2.3.2	パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に求めること	情報セキュリティ関連規程等を査閲し、グループ（共有）パスワードがグループ内だけの秘密に保つようにルール化されていることを確認する。	パスワード管理規則を査閲し、共有パスワードを共有している範囲の人のみに限定することが記載されていた。
7.2.3.3	パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮	情報セキュリティ関連規程等を査閲し、ID の発行毎に 8 文字以上のランダムな初期パスワードが発行され、直ちに変更を要求するようにルール化されていることを確認する。	パスワード管理規則を査閲し、ID の発行毎に 8 文字以上のランダムな初期パスワードが発行され、直ちに変更を要求するよう記述されていることを確認した。

	のパスワードが最初に発行されることを確実にすること	販売管理システムのユーザマニュアルを査閲し、ユーザマニュアル上でもIDの発行毎に8文字以上のランダムな初期パスワードが発行し、それを直ちに変更するようにユーザーに求めていることを確認する。	販売管理システムのユーザマニュアルを査閲し、ユーザマニュアルにIDの発行毎にに8文字のランダムな初期パスワードが発行され、それを直ちに変更するように記述されていることを確認した。
7.2.3.4	パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること	・・・・以下省略	・・・・以下省略

２．２．２　課題

合意された手続については、公認会計士が行う業務以外では実務事例が少ない。しかし、この方法は限定された目的においては、効果的な手法であり、監査の手法の選択肢として利用されることが望ましいといえる。その普及が今後の課題であろう。

２．３　助言型監査

助言型監査とは、対象事象についての客観的な規準が存在することを前提として、入手した十分かつ適切な証拠に基づきその基準への準拠性について対象事象を評価又は測定し、対象事象と規準とのギャップを検出し、独立の第三者として検出事項及び参考意見として改善提言を行うことをいう。

情報セキュリティ監査における助言型監査とは、情報セキュリティのマネジメント又はコントロールの改善を目的として、監査対象の情報セキュリティ対策上の欠陥及び懸念事項等の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を監査意見として表明する形態の監査をいう。

情報セキュリティ監査基準　実施基準ガイドライン

2.1　（前略）情報セキュリティ監査には、（中略）情報セキュリティ対策の改善に役立つ助言を行うことを目的とする監査がある。（後略）

2.4　助言型の監査とは、情報セキュリティのマネジメント又はコントロールの改善を目的として、監査対象の情報セキュリティ対策上の欠陥及び懸念事項等の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を監査意見として表明する形態の監査をいう。（後略）

■　リスク分析の適用

助言型監査において、監査対象を限定して行った場合の監査の有効性の範囲を明確にするために、リスク分析を行うことが望ましい。情報セキュリティ監査は、情報セキュリティのリスクを最小化することを目的とした監査である。監査対象を限定した助言型監査においては、全情報資産のリスクのうち監査対象の情報資産がもつリスクを明らかにすることで、助言に基づく改善効果の範囲を明確にすることが望ましい。この場合、どのようなリスク分析が適切かを検討する必要がある。

２．４　コンサルティング

コンサルティングとは、依頼者からの専門的な事柄の相談に応じることをいう。

情報セキュリティにおけるコンサルティングとは、依頼者からの情報セキュリティのマネジメント又はコントロールの改善に関する課題の相談に応じ、課題の解決を支援する業務をいう。

専門的な事柄の相談に応じること。（三省堂提供「デイリー 新語辞典」）

■　コンサルティング目的とその範囲の明確化

コンサルティング業務では、その依頼者が抱えるリスクのどのような部分に対して支援を行うかの明確化が求められる。依頼内容が多様であり、対象がリスク分析そのものであったり、特定のリスク課題に対する解決であったりすることがある一方で、JIS　X.5080 に基づく情報セキュリティの課題把握と対応という、助言型監査とも言える場合もある。

コンサルティングと保証型監査、合意された手続、助言型監査を峻別する鍵は、三者間関係が存在するか否かである。コンサルティングは、コンサルティング先とコンサルタントの二者しか存在しない。一方、後者は、監査対象、利害関係者（想定利用者、監査報告先)、監査人の三者の関係が存在する。

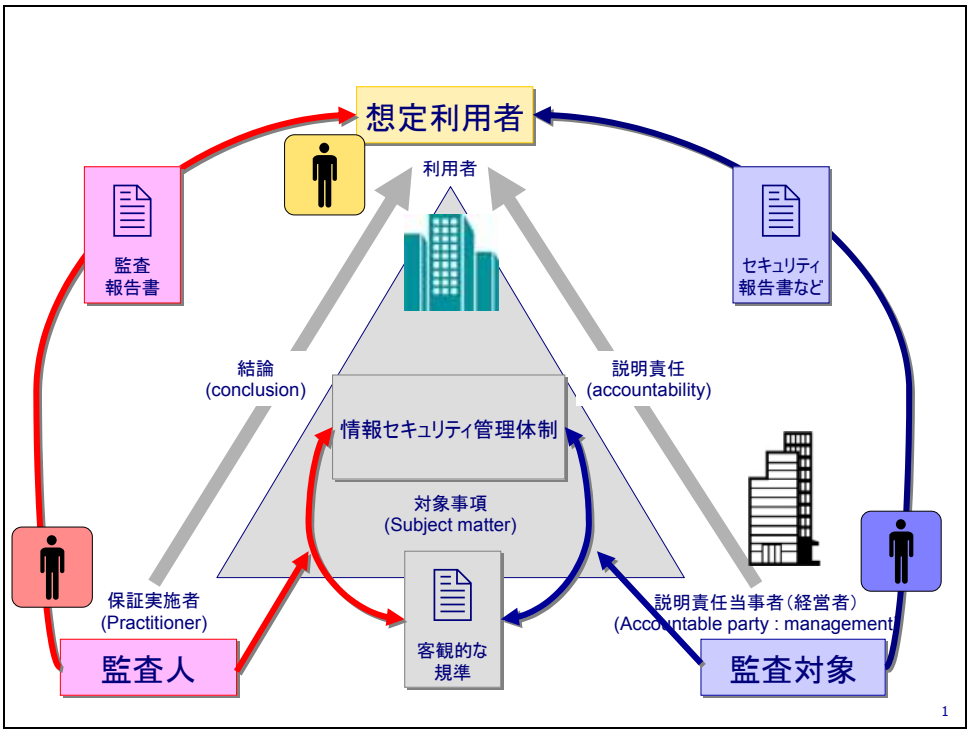


図１：監査の三者関係

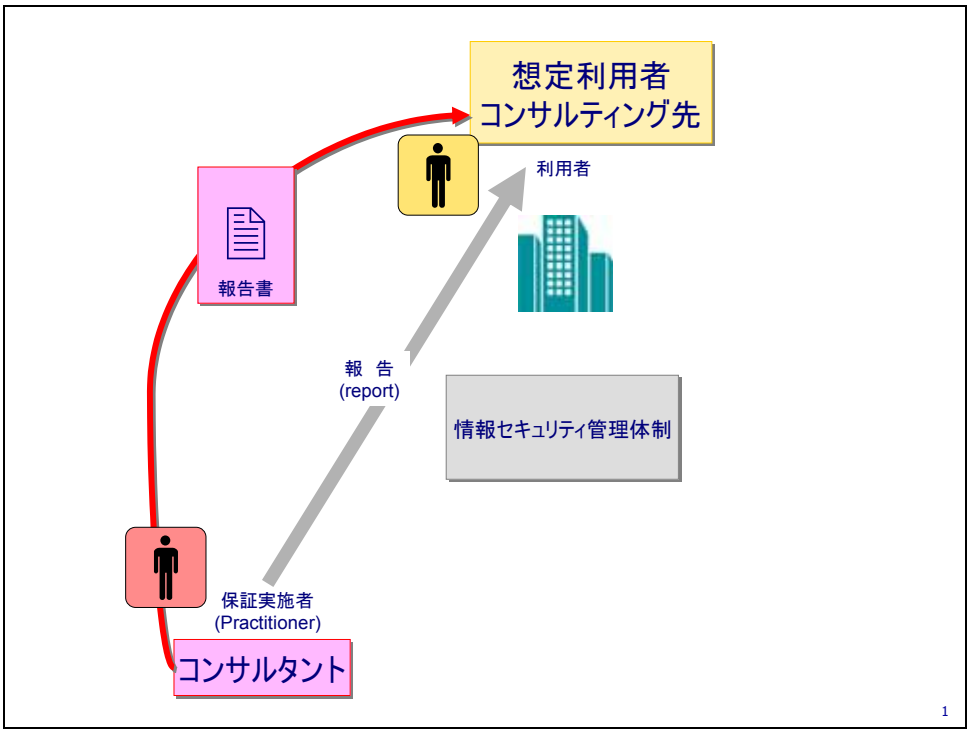


図２：コンサルティング

２．５　今後整理すべき業務形態

■　フォレンジック・オーディット

監査の作業効率を高めるために、もっともリスクの高い部分に監査資源を投入することが望ましい。米国等で議論されているフォレンジック・オーディット　－　対象情報資産のリスク分析を踏まえて、リスクの大きい部分の監査精度を高める方法　－などの導入を検討する必要がある。

註）フォレンジック

「法廷の」「法医学的な」「科学捜査の」という意味を持った形容詞で、コンピュータの世界で「フォレンジック」という言葉を用いる場合は、不正アクセスや情報漏えいといった犯罪行為や、商取引上のトラブルといった訴訟沙汰になりうるリスクに備えて、法廷で用いることができるような証拠を残すための取り組み。

３．情報セキュリティ監査、システム監査、ISMS 審査の異同

情報セキュリティ監査、システム監査、ISMS 審査の相違は、その目的の相違にある。い情報セキュリティ監査は、情報セキュリティに関するリスク・マネジメントの有効性を検証・評価し、保証または助言を与えることが目的である。システム監査は、IT に関わるリスク・マネジメントが有効に作用するための IT ガバナンスが確立しているかを検証・評価し、保証または助言を与えることが目的である。これに対し、ISMS 審査は、対象主体の活動が ISMS の適合性を満たしているかどうかを検証し、それに基づき認証を与えることが目的である。

このように目的は明確に相違するが、これら３つの監査／審査は検証対象が重複しているために、相違が分かりにくい。

システム監査では情報セキュリティも監査対象であり、かつその管理基準は情報セキュリティ管理基準を活用することとされている。このことだけを見れば、情報セキュリティ監査はシステム監査の一部を構成するものである。しかし、情報セキュリティに関しては、個人情報保護等の活動を見れば分かるとおり、情報システム以外も対象としなければならない。その関係は次の図に示すとおりである。目的の相違は、監査対象の範囲の相違でもある。

（参考）http://www.jipdec.jp/security/sysaudit/relations.pdf

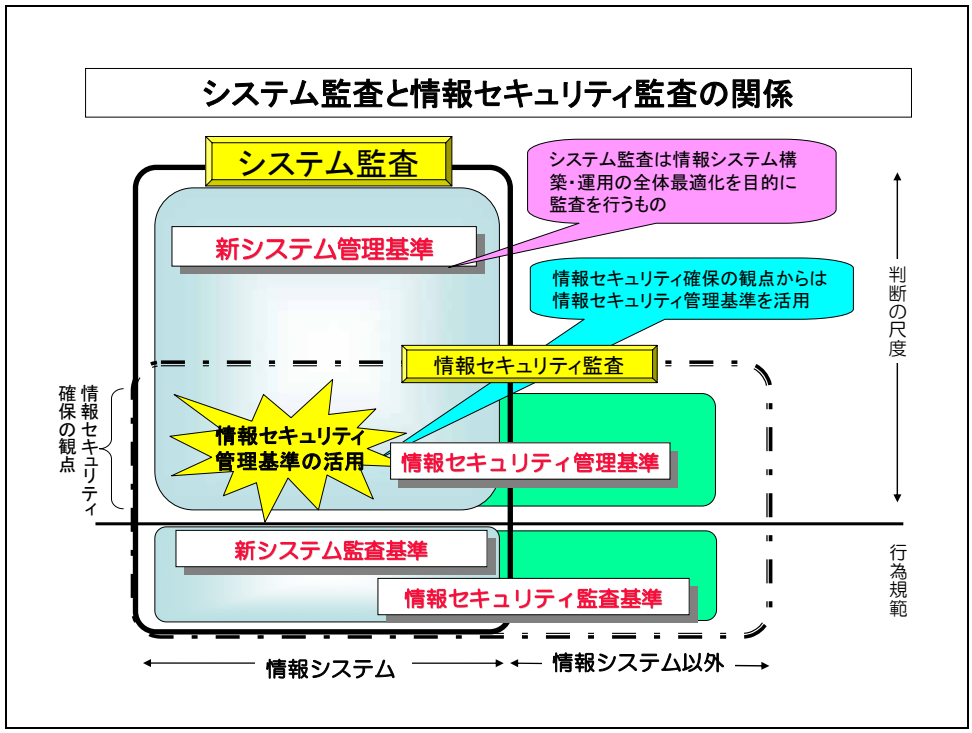


図３：システム監査と情報セキュリティ監査の関係

システム監査と情報セキュリティ監査の関係

- 「システム監査」と「情報セキュリティ監査」はその目的が異なり並立するものである。すなわち、「システム監査」は、企画・開発・運用・保守という情報システムのライフサイクルに従って、特に情報システム構築・運用の全体最適化を目的として監査を行うものであるのに対して、「情報セキュリティ監査」は、情報資産のライフサイクルに従って、情報システム以外の部分も対象として情報セキュリティ確保のための管理・運用を有効に行うことを目的として監査を行うものである。

- また、我が国の状況を見れば、「システム監査」が元来内部監査による助言型監査を前提として成立してきたものであるのに対し、「情報セキュリティ監査」は、情報セキュリティの確保の認識・評価・可視化の必要性という社会的要請から、当初は助言型監査中心の市場になることを想定しているものの、最終的には、保証型監査を中心に行われることを前提として成立しているものである。

- こうして、「システム監査」と「情報セキュリティ監査」とは、目的及びその成り立ちが異なり、ユーザ（被監査主体）のニーズ及び要請に応じて適切に選択されるべきものである一方で、「システム監査」においても情報セキュリティ確保の観点からの監査項目を、その一環として加えていくことがあり得る。しかしながら、情報セキュリティ確保の観点からの監査は、基本的には「情報セキュリティ監査制度」を基軸として運用を行っていくことが要請される。なお、「システム監査」において情報セキュリティ確保の観点からの監査項目を加えて行う場合においては、「情報セキュリティ管理基準」を活用して実施することが適切である。

- 以上の整理を踏まえ、今般の「システム監査基準」の改訂に当たっては、新「システム管理基準」及び新「システム監査基準」の前文に上記の趣旨を盛り込むとともに、新「システム管理基準　６．情報セキュリティ」に「その他詳細な情報セキュリティ管理項目に関しては、情報セキュリティ管理基準を活用すること」との項目を明記しているところである。

（出典）経済産業省　「システム監査と情報セキュリティ監査の関係」

ISMS 審査と情報セキュリティ監査の類似性は、ISMS が対象とする情報セキュリティ・マネジメントの基準が、情報セキュリティ管理基準のマネジメント部分と重複があることである。このため、ISMS 審査を行っている立場からは、情報セキュリティ監査は審査と同じ活動であるように見える。しかし、経営層が情報セキュリティに関するリスクを把握し、対応をとるという組織的なマネジメントの行為を審査することと、それが末端まで確実に浸透し、実施され、その結果を末端の担当者が認識し、リスクを経営層にフィードバックできるという担当者レベルの実施能力を検証することには、相違がある。米国の専門家には、前者をアセスメント（Assessment)、後者をバリデーション（Validation）と呼び、その相違を明確にした上で、それぞれに適する方法を採用する人もいる。この用語を用いれば、ISMS 審査はアセスメント主体であり、情報セキュリティ監査は監査目的によって、アセスメント主体、バリデーション主体、あるいは両者すべてを行うものといえる。情報セキュリティ監査のうちのアセスメント主体のものは、ISMS 審査の検証とほぼ同等の検証作業となる。

３．１　情報セキュリティ監査

３．１．１　目的

情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと

情報セキュリティ監査基準
情報セキュリティ監査の目的

情報セキュリティ監査の目的は、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにある。

情報セキュリティのマネジメントは第一義的には組織体の責任において行われるべきものであり、情報セキュリティ監査は組織体のマネジメントが有効に行われることを保証又は助言を通じて支援するものである。

３．１．２　監査の種類

保証型監査、合意された手続、助言型監査

３．１．３　判断の尺度

原則として情報セキュリティ管理基準となる。

しかし、監査の要請又は目的によって、情報セキュリティ管理基準以外の適切な管理基準等を用いることができる。

また、監査の要請又は目的、ないしは被監査側の特性またはリスクの程度等を考慮して、情報セキュリティ管理基準の一部の管理項目を判断の尺度とすることができる。

情報セキュリティ監査基準

前文

（前略）情報セキュリティ監査は、本監査基準の姉妹編である情報セキュリティ管理基準を監査上の判断の尺度として用い、監査対象が情報セキュリティ管理基準に準拠しているかどうかをという視点で行われることを原則とする。（後略）

情報セキュリティ監査基準　実施基準ガイドライン

1.4　「情報セキュリティ監査基準」に従った監査においては、本監査基準と姉妹編をなす「情報セキュリティ管理基準」を監査上の判断の尺度として用いることを原則とする。ただし、情報セキュリティ監査の要請又は目的によって、「情報セキュリティ管理基準」以外の適切な管理基準等を、監査上の判断として用いることもできる。

1.6　（前略）ただし、情報セキュリティ監査の要請又は目的、ないしは被監査側の特性又はリスクの程度等を考慮して、当該管理基準の一部の管理項目（例えば、外部委託契約にかかわる管理項目等）を監査の対象とすることができる。（後略）

1.8　情報セキュリティ監査において、「情報セキュリティ管理基準」以外の管理基準を用いる場合には、監査の目的等に照らして、管理基準としての体系性、標準性、適用可能性等について、情報セキュリティ監査人は慎重に検討しなければならない。

1.9 情報セキュリティ対策に係る管理項目を含む管理基準等で政府機関が公表している国内基準には、経済産業省「システム監査基準」、「情報システム安全対策基準」、「コンピュータウイルス対策基準」、「コンピュータ不正アクセス対策基準」、総務省「情報通信ネットワーク安全・信頼性基準」、警察庁「情報システム安全対策指針」等がある。

1.10　情報セキュリティ対策に係る管理項目を含むその他の管理基準等で国際的に認知度が高いものに、内部監査協会（IIA）の「eSAC」、情報システムコントロール協会（ISACA）の「COBIT」、アメリカ公認会計士協会（AICPA）/カナダ勅許会計士協会（CICA）の「Trust 業務原則及び規準」などがある。

1.11 情報セキュリティ監査における監査上の判断の尺度として、上記 1.9 及び 1.10 に限らず、各種公的機関又は監査サービス会社等で作成した管理基準等、あるいは組織体が独自に定めた管理規定（情報セキュリティ基本方針を含む）、CPS（認証局運用規程）、SLA（サービス水準合意書）等を用いることを妨げるものではない。ただし、組織体が定めた情報セキュリティ基本方針、CPS、SLA 等については、当該規定類の適切性に係る保証又は助言が情報セキュリティ監査の目的とされることもあり得る点に留意する。

３．１．４　保証型監査の場合の保証水準

規定されていない。

会計監査の保証水準を高水準（合理的な保証）とした場合、情報セキュリティ監査では、高水準（合理的保証）から、中水準（限定的保証）までとりうる。

保証型監査を推進する上で保証水準を定義することが重要である。

３．２　システム監査

３．２．１　目的

組織体の情報システムにまつわるリスク対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスの実現に寄与すること

システム監査基準

システム監査の目的

システム監査の目的は、組織体の情報システムにまつわるリスク対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスの実現に寄与することにある。

３．２．２　監査の種類

保証型監査、合意された手続、助言型監査

システム監査基準の枠組みでは、合意された手続についての言及はないが、理論的にはありえると考える。

３．２．３　判断の尺度

原則として情報システム管理基準。ただし、情報セキュリティ監査については、原則として情報セキュリティ管理基準を活用することが望ましい。

情報システム監査基準

前文

（前略）情報システム監査は、本監査基準の姉妹編である情報システム管理基準を監査上

の判断の尺度として用い、監査対象が情報システム管理基準に準拠しているかどうかをという視点で行われることを原則とする。(後略)

実施基準

６．情報セキュリティ監査

情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。

３．２．４　保証型監査の場合の保証水準

規定されていない。

会計監査の保証水準を高水準（合理的な保証）とした場合、情報セキュリティ監査では、高水準（合理的保証）から、中水準（限定的保証）までとりうる。

保証型監査を推進する上で保証水準を定義することが重要である。

３．３　ISMS 適合性評価制度

３．３．１　ISMS 審査をうけることの目的

組織体が構築した ISMS が ISMS 評価基準に適合していることを、独立した ISMS 審査機関が審査することにより、利害関係者に対して、組織体が ISMS 評価基準に適合した ISMS を構築していることについての説明責任を果たすこと。

JIPDEC　ISMS 適合性評価制度の概要（2003 年 5 月 30 日）

ISMS 認証を取得するメリット

- 対外的には、情報セキュリティの信頼性を確保できる。
  - 顧客や取引先からのセキュリティに関する要求事項の満足など。
- 内部的には、事業競争力の強化につながる。
  - 入札条件や電子商取引への参加の条件整備など。

３．３．２　監査の種類

保証型監査

３．３．３　判断の尺度

ISMS 評価基準

（参考）

JIS Q 19011:2003 品質及び／又は環境マネジメントシステム監査のための指針

6.2.2　（前略）監査基準*は，それに対する適合性の判断のための相手として使用されるもので，適用される方針，手順，規格，法律及び規制，マネジメントシステム要求事項，契約上の要求事項又は業界の行動規範を含めてもよい。（後略）

* : 監査基準は、Criteria すなわち、監査の判断尺度のことを意味している。

３．３．４　保証水準

中水準（限定的保証）であると考えられる。 明確には規定されていないが、会計監査の保証水準を高水準（合理的な保証）とした場合、 ISMS 適合評価制度における適合性評価では、中水準（限定的保証）であると考えられる。

JIS Z 9362-1996 「品質システム審査登録機関に対する一般要求事項」の適用に関する IAF ガイダンス Issue3 (IAF GD2:2003)

従業員数（人）		初回審査の審査工数（人日）
1	10	2
11	25	3
26	45	4
46	65	5
66	85	6
86	125	7
126	175	8
176	275	9
276	425	10
426	625	11
626	875	12

従業員数（人）		初回審査の審査工数（人日）
876	1175	13
1176	1550	14
1551	2025	15
2026	2675	16
2676	3450	17
3451	4350	18
4351	5450	19
5451	6800	20
6801	8500	21
8501	10700	22

参考文献

1. 経済産業省　告示　情報セキュリティ監査基準
2. 経済産業省　情報セキュリティ監査研究会　情報セキュリティ監査基準実施基準ガイドライン
3. 経済産業省　情報セキュリティ監査研究会　情報セキュリティ監査基準報告基準ガイドライン
4. 経済産業省　公表　システム監査基準
5. 企業会計審議会　財務情報等に係る保証業務の概念的枠組み　2004 年 11 月 19 日
6. 日本公認会計士協会　保証業務フレームワーク検討ＰＴ報告書　公認会計士が行う保証業務に関するフレームワーク（試案）平成 16 年 7 月 6 日
7. 日本規格協会　JIS Q 19011:2003 品質及び／又は環境マネジメントシステム監査のための指針
8. 日本適合性認定協会　JIS Z 9362-1996 「品質システム審査登録機関に対する一般要求事項」の適用に関する IAF ガイダンス Issue3 (IAF GD2:2003)

その他参考となる文献

保証型監査関係

1. International Federation for Accountants (IFAC), International Standard on Assurance Engagements (ISAE) 3000 Assurance Engagements Other Than Audits or Reviews of Historical Financial Information
2. American Institute of Certified Public Accountants (AICPA) Profetional Manual Attestation Standards (AT) Section 101 Attest Engagements
3. American Institute of Certified Public Accountants (AICPA) Profetional Manual Attestation Standards (AT) Section 601 Compliance Attestation

合意された手続関係

1. International Federation for Accountants (IFAC), International Standard on Related Services (ISRS) 4400 Engagements to Perform Agreed upon Procedures Regarding Financial Information
2. American Institute of Certified Public Accountants (AICPA) Profetional Manual Attestation Standards (AT) Section 201 Agreed-Upon Procedures Engagements

コンサルティングサービス関係

1. American Institute of Certified Public Accountants (AICPA) Statement on Standards for Consulting Services

第１編　第２部　技術部会ＷＧ２

具体的な技術的情報セキュリティ管理基準の検討

平成 17 年 3 月 31 日

第1編　第2部　目次

１．本報告書の背景と目的 39
２．アプローチ 39
添付資料 A　監査対象の想定モデル
1 業務定義 41
2 組織 41
3 物理的環境 41
4 サービス概要 42
5 ＩＤＣサービス 42
6 システム（サービス提供側のインフラ） 51
7 情報センターの物理的環境およびセキュリティ 53
8 データ 60
9 受託システム例 61
10 Ｓ社のネットワーク環境 63
11 Ｓ社の各サービスにおける情報資産 64
添付資料 B　IDC サービスにおける情報セキュリティ管理基準
マシンレンタル（ハウジング）サービス 69
インターネット接続サービス 95
監視サービス 121
ファシリティ関連 147

技術部会ＷＧ２ 参加及び報告書作成メンバーリスト（敬称略）

（ＷＧ２リーダ）

菅谷　光啓　　NRI セキュアテクノロジーズ株式会社 情報セキュリティ調査室

（ＷＧ２メンバー：氏名５０音順）

池田　秀司　　株式会社ディアイティ セキュリティビジネス推進室
生駒　勝治　　ニッセイ情報テクノロジー株式会社 ビジネスソリューション事業部
上田　潤　　日本ユニシス株式会社 情報システム部
薄田　利夫　　株式会社イトーキ 施設別事業部
北澤　麻理子　ドコモ・システムズ株式会社 セキュリティサービス部
木村　尚亮　　NRI セキュアテクノロジーズ株式会社 事業開発部
小林　伸太郎　三菱電機株式会社 社会ｅソリューション事業所 社会システム部
住谷　清　　株式会社コアサイエンス システム開発部

関　克彦　　KPMG ビジネスアシュアランス株式会社 IRM 事業部
田村　仁一　監査法人トーマツエンタープライズ リスクサービス部
辻　信行　　中央青山プライスウォーターハウスクーパース・フィナンシャル・アンド・リスク・マネジメント株式会社
成島　佳孝　株式会社日立製作所 セキュリティソリューション推進本部
広口　正之　株式会社インフォセック リスクコンサルティング事業本部
福原　幸太郎 株式会社オリエントコーポレーション 検査部
増田　進　　株式会社電算　セキュリティ監査事業部
横川　英之　みずほ情報総研株式会社 生産技術部

１．本報告書の背景と目的

情報セキュリティ監査は、約９６０項目にも及ぶ情報セキュリティ管理基準を基に、対象とする情報資産や組織の規程、関連法令やその他規程等各組織における個別の事情に鑑みて、その組織や監査対象毎に管理項目を定め、その各項目を監査項目として読み替えチェックリストを作成する（下図参照）。

経済産業省から示されている管理項目は一般的に使えるよう、抽象度の高い表現で記述されている。しかしながら、監査対象を特定した場合には、この組織毎の個別の管理基準はより具体化された表現となり、何をどう監査すべきかがより明確になるような表現となるはずであるが、これまでそうしたより具体的な管理項目は政府あるいは他の組織からは示されていない。

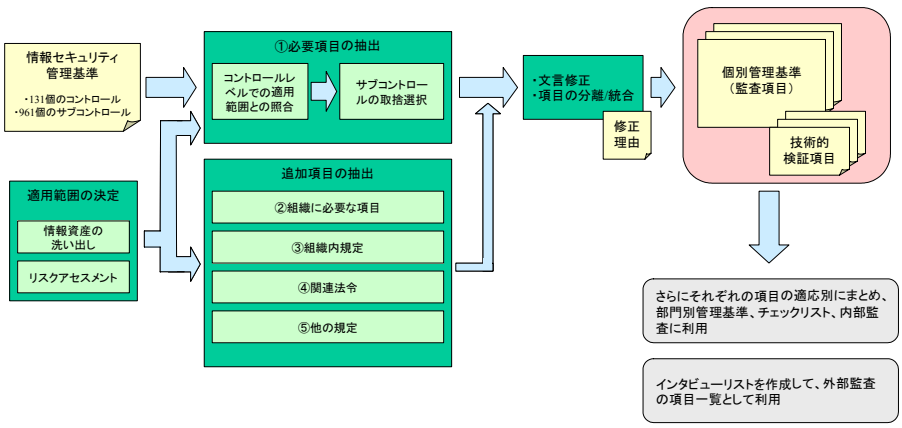
本 WG では、こうした問題意識に基づいて、特定のサービスを例に取り上げ監査対象を特定した場合、９６０あまりの一般的管理項目の意を汲みながらサブコントロールのレベルでどのような記述であるべきかを検討した。

２．アプローチ

例に取り上げる対象としては、インターネットデータセンター（以下、IDC）のサービスとした。IDC のサービスには一般的に、以下のようなサービスが存在する。

- ホスティングサービス
- ハウジング（およびマシンレンタル）サービス
- 監視サービス
- バックアップサービス
- 大量印刷サービス
- イントラネット接続サービス

図 1-1　個別管理基準の作成



また、セキュリティに関連するサービスとして以下のようなサービスを提供する IDC も増えており、以下のようなサービスが提供されている。

- ウイルスチェックサービス
- ファイアウォール サービス
- 不正侵入検知/防御サービス
- インターネット VPN サービス
- URL フィルタリングサービス
- 認証サービス

本 WG での検討対象としては、ホスティング、ハウジング（マシンレンタル）、監視のサービスを取り上げた。またこれに加え、IDC におけるサービスの基礎となるファシリティについての管理基準の策定も行った。

また、管理基準の項目の中にはマネージメント的なコントロール（サブコントロール）も多々存在するが、マネージメントの管理基準は監査対象の違いによる記述の違いが技術的なものに比べて少ないと予想されるため、本 WG での活動は技術的な管理基準に焦点を当てた。

このために、本 WG での活動は

① モデルの策定
② 技術的管理基準の抽出
③ サブコントロールの読替

というステップで実施した。

本報告書では、添付資料 A に、このモデルを具体化し、添付資料 B に上記の４つの各サービス（ホスティング、マシンレンタル、監視のサービスとファシリティ）について、技術的な項目に関してサブコントロールの読替えをおこなった管理基準を示す。

添付資料 A　監査対象の想定モデル

1 業務定義

モデルは、企業グループの情報システム子会社とする。

グループの親会社をP社(Parent)、情報システム子会社をS社(System)とする。S社は、P社の情報システム部門が独立してできたため、P社の情報システムの構築、ソフトウェア開発、システム運用を手がけている。S 社の社員数は約 100 名である。この他に協力会社の社員が約 30 名、常駐している。親会社の P 社にも、情報システムの企画部門は存在しているが、情報戦略を立案するのが中心で、具体的な作業はS社が実施している。

（P 社企業グループの業種は、特定する必要が出てきた場合に特定することとする。）

P 社企業グループには、グループ関連会社が数十社存在しており、S 社は、親会社の P 社だけでなく、グループ各社の情報システムの構築、開発、運用の一部も手がけている。グループ各社については、情報システムの選択は、各社に任されており、S社を起用しない会社もある。グループ各社については、さまざまな利用形態があるが、ウェブサーバや基幹業務システムのホスティング・サービス、ハウジング・サービスなどが中心である。S 社としては、競争力の確保と、売上拡大のために、グループ外の業務比率を今後高めていきたいと考えている。

2 組織

S社の組織は、総務部、企画部、人事部、営業部、システム開発部、システム運用部に分かれている。システム開発部は、システム構築、ソフトウェア開発を行う。システム運用部は、ホスティング・システム、ハウジング・システム、サービス提供システムの運用を行う。

3 物理的環境

P社の情報システムは、防災上の観点と、地価の点から、東京郊外の情報センターに設置されている。この場所は、地盤が固く、付近に活断層が無く、水害の恐れも少ないという立地条件から選定された。都心から約 30km、電車で一時間、自動車でも約一時間の距離である。周囲の道路は道幅も広く、建物の間隔も広いため、近隣火災の延焼の恐れは少ない。また、徒歩 5 分以内に大きな公園があり、避難場所として指定されている。

情報センターは、5階建ての建物であり、1F が食堂と来客者用会議室、オフィスフロア、2F がオフィスフロア、3F～5F がマシン室フロアである。一部のマシン室には、運用要員のためのオフィスが設けられている。

平日昼間（9:00～17:30）は、受付が入退場を管理するが、それ以外の平日夜間、土日祝日は、警備員が入退場を管理している。外部者の入退場は、事前の届け出と、台帳への記入、社員証等の身分証の提示、社員のエスコートが必要である。マシン室への入退場は、IC カードシステムによって管理されている。外部者が作業する場合で、社員が常時エスコートできない場合には、IC カードを

申請により貸与する。エレベータの手前にセキュリティドアがあり、やはりICカードシステムによって管理されている。

情報センターが機能しなくなったときのバックアップ・センターとしては、23区内にある、旧情報センターが使われることになっている。ここは、現在、開発用の拠点として使われているが、バックアップ・センターとしても機能するように考えられている。

情報センターの物理的な配置およびセキュリティ対策については、7節を参照。

4 サービス概要

.4.1 システム構築

情報システムの開発を実施するが、最初から最後まですべてをS社だけで実施することは少なく、ハードウェア構成設計やネットワーク構成設計を外注したり、ハードウェアベンダーに設計込みで発注したりしている。開発対象はP社のシステムやネットワークが多いが、グループ各社やグループ外企業の開発も請け負っている。

.4.2 ソフトウェア開発

S社は、ソフトウェアを開発するが、最初から最後まですべてをS社だけで実施することは少なく、ソフトウェアを外注したり、派遣者、出向者を受け入れたりしながら業務を遂行している。開発対象はP社のシステム上で稼働するソフトウェアが多いが、グループ各社やグループ外企業のソフトウェアも開発している。

.4.3 ＩＤＣサービス

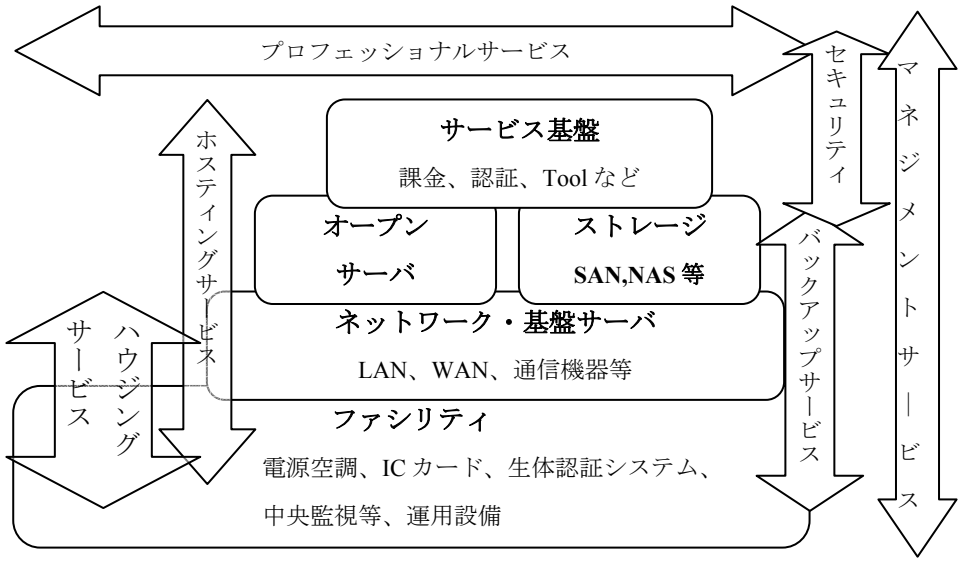
S社は、情報センター内のシステムを運用している。障害発生時の障害原因の切り分け、メイン系とバックアップ系の切り替え、ベンダーへの連絡、修理済みのマシンの復帰、システムファイル、データファイルのバックアップ、バックアップ・テープの架け替え、稼働状況のモニター、運用報告書の作成、問題点の報告と改善提案などを実施している。ホスティング・サーバに関しても、同様な運用を実施している。ハウジング・サービスのサーバについては、基本的に顧客が運用を実施するが、電源のリセット程度の作業であれば、顧客からの依頼で実施することもある。

また、P社では、インターネットメールではなく、専用メールシステム(Domino/Notesのイメージ)を使用しており、S社はこうしたサーバの構築や運用も実施している。

さらに、P社や、グループ各社の個人用PCのトラブルシュート、社員用ヘルプデスク機能もS社の分担範囲である。

サービスの詳細は次節を参照。

5 ＩＤＣサービス



.5.1 サービスの概要

サービスは IDC での運用の基本的なスタイルを選択することが必須である。
基本メニューを選択し、その上に様々なサービスをソリューション（後述）として追加することが可能。

● 基本メニュー

■ ハウジングサービス

「潤沢なネットワーク資源の提供とセキュアな物理的な環境の提供」

機器設置スペース提供

インターネットへのネットワーク提供

■ ホスティングサービス

「スケールアップ可能なサーバの提供と必要に応じたソリューションの提供」

機器設置スペース提供、サーバ(ハード)提供、サーバ上のミドルウェアを提供

ネットワーク接続機器の提供

■ 接続サービス

「企業のインターネット接続機能を提供」

ネットワーク接続機器の提供（Firewall、IDS）

参考：基本メニューの整理

提供可能機能	詳細	ハウジング	ホスティング	接続
ファシリティ	電源（冗長化も可能） ラック 設備（空調、防災・消化、防火等） 入退館室管理、監視（物理的）	○	○	△

マシンレンタル	ハードウェア(サーバ)	PC サーバ UNIX 冗長構成の為の Load Balancer も提供可能	×	○	×
	ソフトウェア（運用を含む）	ソフトウェア OS　Windows、商用 UNIX（Solaris,HP-UX）、Linux（Redhat） ミドルウエアソフト UNIX、Windows でそれぞれ 1 種づつ用意（SMTP、HTTP、FTP、DBMS） その他 Perl 等の Tool 群もセットで推奨環境を用意	×	○	×
	ハードウェア(ネットワーク)	回線 センター指定機種のみ提供 ルータ、S/W	△	○	○
接続サービス	インターネット接続	DNS 運用（1 ドメインを標準）、電子メール 汎用の F/W での簡単なポート制御可能	○	○	○

○　提供可能

△　一部提供可能

×　提供不可

● オプションサービスについて

選択対応表

基本サービス	サービス概要	基本サービス		
		外部ネットワーク接続サービス	ホスティングサービス	ハウジングサービス
運用マネジメントサービス	監視サービス （稼動、性能）監視、管理を行い、通知を行う	△	○	△
	バックアップサービス 大容量のデータ保管環境を提供し、バックアップなどの環境を提供するサービス	○	○	△
	大量印刷サービス 業務に必要な帳票印刷を、高速プリンターにて、短時間で実施するサービス	○	○	○
	イントラネット接続サービス 専用のネットワークをハウジングネットワークへ接続	○	○	△
セキュリティソリューションサービス	ウイルスチェックサービス 中継時にメールに添付されたウイルス感染ファイル、メールを検出・削除)	○	○	○
	ファイアウォール サービス ファイアウォールを提供し サーバ、ネットワークを安全に運用	○	○	○
	不正侵入検知/防御サービス 不正侵入による攻撃、情報漏洩、ワームなどの 検知（IDS.IDP 機能）	○	○	○
	インターネット VPN サービス VPN 機器を使用したインターネット VPN サービス。 ファイアウォール S と兼用も可能	○	○	○
	URL フィルタリングサービス Web アクセスなどを URL によるフィルタリングを行うサービス	○	○	○
	認証サービス 限定会員サービスを行うなど、認証に必要な認証サーバ機能を提供する。	○	○	○

○　提供可能

△　一部提供可能

×　提供不可

想定モデルの監査対象として組み入れて考えるサービス
（インターネット VPN サービスは接続サービスに入れて考える）

.5.2 サービスの詳細

以降はオプションとなる付加サービスの詳細について延べる。

1) 運用マネジメントサービス

i) 監視サービス

（稼動、性能）監視、管理を行い、通知を行う。

データセンターにて稼動しているシステムに対して２４時間３６５日ネットワーク、サーバ等の監視を行う。

障害発生時などには、自動的に携帯電話、ｅメール等に自動的に発報を行いサービスの停止を発見し、システムの安定稼動の情報を提供。

（障害履歴情報はデータベースに蓄積され、月次にて報告を行う。）

■ 監視サービス

Ｐｉｎｇコマンド等によりネットワーク、サーバ機器の接続状況監視 を行う

■ プロセス監視サービス

サーバ上で稼動しているプロセスの稼動監視 を行う

■ ログ監視サービス

サーバ上でログファイルに出力された特定の文字列(エラーメッセージ等)の監視

■ リソース監視サービス

サーバ上のＤｉｓｋ、ＣＰＵ、メモリの使用率の閾値による監視

■ アプリケーション監視サービス

ＥＲＰパッケージ等のアプリケーション稼動監視

■ パフォーマンス監視サービス

Web アプリケーション等、アプリケーションの実際の応答確認を定期的に行い、サービスが確実に提供されているかを監視。

また、応答時間を確認することで、アクセス増による応答速度の低下を監視する。

(SMTP サーバ、FTP サーバ等も対応可能)

例：Web サーバへ指定した URL について、ファイルなどが取得可能か。

■ 総合監視サービス

お客様のシステムからの通報対象となるアラートを監視（前述のサービスによる監視のアラート）し、自動的に通知するとともに通報履歴情報を管理

※上記サービスには SNMP を使用するため、サーバへのエージェントソフトのインストールを必要とする場合がある。

ii) バックアップサービス

大容量のデータ保管環境を提供し、バックアップなどの環境を提供する。

また、外部メディアなどへの保管作業も自動的に行う。

■ データバックアップサービス

DB やアプリケーションのデータをバックアップ。

増分バックアップやフルバックアップ、世代数や保管期限など柔軟な設定が可能。

■ システムバックアップサービス

サーバ/OS 障害等のシステム障害に備え、OS 部分のシステムディスクのバックアップを行うサービス。

OS へのパッチ適用時、OS バージョンアップなどの構成変更時に行うバックアップ

■ 隔地保管サービス

バックアップサービスを使用して、バックアップしたデータを、当社の別センターに隔地保管することが可能。

※運用しているサーバとの間に専用のネットワークを敷設し、ネットワーク経由でのデータの保管を実施する。

その際には、対象サーバには専用のネットワークインタ-フェースを用意する必要がある。

※バックアップサーバとの間には、ファイアウォールによるアクセス制御を行う。

従って、同様のサービス提供を受けている他のサーバへはアクセスは不能である。

iii) 大量印刷サービス

以下のような印刷、郵送物の発送業務を行う。

■ 事前印刷用紙への印刷サービス

レーザプリンターによる多様な用紙への高速、大量印刷

・罫線・ロゴ等をカラー印刷した用紙への印刷

・圧着ハガキ・宛名ラベルを使用した印刷

■ 汎用用紙への印刷サービス

レーザプリンターによる汎用（白紙）用紙への高速、大量印刷

・オーバーレイ(罫線・枠等)をデータと共にプリンターにて印刷

・各種明細・統計資料等、社内利用資料の大量印刷

■ バーコード印刷サービス

レーザプリンターによる多種バーコードの印刷

・カスタマーバーコードの印刷

・料金代理収納用バーコード(1 段化 UCC/EAN-128)の印刷

■ PDFファイルの大量印刷サービス

レーザプリンターによるオープン系データの大量印刷

・オープン系システムで作成した大量の帳票(PDF)を印刷

■ 複写用紙への印刷サービス

インパクト・プリンターによる多様な用紙への大量印刷

・感圧紙等による、大量複写(コピー)印刷

■ CD-R などへのメディア焼付け

iv) 不正侵入検知/防御サービス

不正侵入による攻撃、情報漏洩、ワームなどのネットワークセキュリティ犯罪から企業の情報資産を防御

不正侵入検知/防御サービスは、I 社が提供のネットワーク型不正侵入検知/防御アプライアンス製品を用いて、お客様のネットワークを最新かつ深刻な脅威から防御する。

当社データセンターにおける物理的なセキュリティと不正侵入検知/防御サービスを有機的に統合し、企業の情報資産を守る真の防御を実現します。また、当社ファイアウォールサービスと併用することにより、セキュリティインシデントへの迅速な対応が可能。

セキュリティに関する連携は外部のセキュリティベンダーの I 社 SOC と提携し、分析を行う。

	不正侵入検知サービス	不正侵入防御サービス
検知・防御機能	侵入検知を行うことを主目的	侵入検知と同時に自動防御を
設置形態	ステルス型 HUB/Switch/TAP 等が必要	インライン型 ネットワーク構成を変更することなく設置が可能

※IDS は冗長構成とし、障害時にも対応可能とする。

v) ファイアウォール サービス

データセンター設置のファイアウォールでサーバを安全に運用

月次でのレポートなどは専用 Web にて提供する。

専用 Web では以下のようなファイアウォール統計全般が参照できる。

・許可/拒否された接続数

ホスト別利用状況/プロトコル別利用状況/利用ホスト別プロトコル利用状況）

・拒否された通信情報一覧

・サービス別

通信量グラフ（アクセス先ウェブ利用状況一覧/

メール送信元・送信先一覧/FTP 通信リスト一覧/Telnet 通信リスト一覧）

・時間/曜日別

送受信通信量グラフ

	小規模	中規模	大規模
ハードウェア	N 社 IP シリーズ他		
クライアント数	50/100/250/500/無制限（サービス開始後のアップグレードも可能）		
イーサポート	10/100 Ethernet		10/100 Ethernet Gigabit Ethernet
ソフトウェア	CP 社製 Firewall　ソフトウェア J 社　Firewall ソフトウェア		
サービス内容	● セキュリティポリシー検討支援 ● ファイアウォール監視・故障対応（SLA 付き） ● 月 10 回までのポリシー設定変更（10 回目以降は別途） ● ファイアウォールソフトウェアのアップデート ● アクセスログをウェブ上でレポート ● インタフェースの追加 ● ホットスタンバイ ● 緊急ポリシー変更		

vi)　インターネット VPN サービス

VPN 機器を使用したインターネット VPN サービス。

ファイアウォールと兼用可能でサービス内容は以下のようになる。

- 専用・・・ VPN 接続用として利用可能。(ファイアウォールは別途設置)
- マルチ・・ VPN 接続機器とファイアウォール機能を備える 1 台の VPN 機器でインターネット接続と VPN 接続機能を同時に備える。

ハードウェア	NS-5GT		NS-25	NS-50	NS-204
ライセンス数 （許容セッション数）	10	無制限	無制限	無制限	無制限
LAN 間 VPN トンネル数 （拠点数）	最大 10 *2		最大 25	最大 100	最大 1,000
リモート VPN トンネル数 （クライアント数）			最大 100	最大 400	最大 1,000
ポート数	イーサネット×5 （LAN 側×4/WAN 側×1）		イーサネット×4 （LAN/DMZ/WAN/ホットスタンバイ用）		
VPN スループット （3DES）	20Mbps	20Mbps	20Mbps	50Mbps	200Mbps
ファイアウォール ポリシー数	100	100	500	1,000	4,000

vii) ウイルスチェックサービス

インターネットと顧客に提供するホスティング、ハウジングの環境の間で、ウィルスチェックゲートウェイにより、メールおよびＨＴＴＰアクセスでのウィルス・ワーム等の有害ソフトウェアを検出し、削除するサービス。

特徴として、

・メールはHTTPはインターネットと顧客環境側の双方向の通信に対応
・多種類の圧縮ファイル/エンコードに対応
・ウイルスチェックサーバには負荷分散システムを採用
・ウイルスチェックは、当社が運用する SMTP 中継サーバ上で実施（自社でメールサーバを運用している場合でも、当社のインターネット接続サービスをご利用いただくことにより、本サービスをご利用可能）

viii) URL フィルタリングサービス

Web アクセスなどを URL によるフィルタリングを行うサービス。

対応プロトコルは、HTTP, HTTPS。

■ カテゴリ一覧

規制対象となる URL は、25 の大分類と、76 の小分類を行って、データベースに登録され、これを元に小分類毎に「許可」「遮断」「書き込み規制」のフィルタリング動作を設定できます。

メインカテゴリ一覧： 不法、主張、アダルト、セキュリティ、出会い、金融、ギャンブル、ゲーム、ショッピング、コミュニケーション、ダウンロード、職探し、グロテスク、話題、成人嗜好、オカルト、ライフスタイル、スポーツ、旅行、趣味、宗教、政治活動・政党、広告、ニュース 等

■ スケジュール設定

「土日祝日用」「平日業務時間用」「平日昼休み用」等、スケジュールにより、異なる Web アクセスルールの設定が可能。

■ 任意の URL を登録可能

DB 登録済みカテゴリへ、ユーザ独自に URL を追加登録する機能を保有。

また、以下のような許可ルールが利用可能。

「常時許可カテゴリ（ホワイトリスト）」

「常時遮断カテゴリ（ブラックリスト）」

「常時書き込み規制カテゴリ」

■ ブラウザに規制画面を表示

Web ページへのアクセスがフィルタによって遮断もしくは書き込み規制された場合、規制されたことを示すメッセージをブラウザに表示。

画面のメッセージはカスタマイズ可能。

■ ログ取得機能

URL フィルタリングソフトのログおよびプロキシサーバの全てのアクセスログを提供いたします。

URL フィルタリングソフトのログには、Allowed/Proxied（許可）・Blocked（遮断）または BlkPst（書き込み規制）が記録され、各カテゴリに属する URL へのアクセスに関しては、該当カテゴリ情報を記録。

プロキシサーバと URL フィルタリングソフトのログファイルは、管理サーバより参照及びダウンロードが可能。ログの保存期間は最大 2 週間。

ix) **認証サービス**

会員サービスに認証サービスを利用する際にデータセンターに設置サーバにて利用可能とする。

以下のような認証の手段を提供する。

・ワンタイムパスワード

・電子証明書

・ID/パスワード

但し、電子証明書は第三者機関である、V 社の証明書を利用するものと、当社 CA の発行する独自のものの 2 タイプを用意。

6 システム（サービス提供側のインフラ）

P社の古くからのシステムは、汎用大型コンピュータを中心とする、レガシーシステムで構築されていたが、現在はもう使用されていない。最近になって構築されたシステムは、ダウンサイジングの流れを受け、サーバ、PC をベースとした、クライアント・サーバシステムで構築されているものが多い。また、インターネットを利用したシステムとして、ウェブサーバや、メールサーバを立てているシステムも存在する。

グループ各社に対するサービスは、ウェブサーバや基幹業務システムのホスティング・サービス、ハウジング・サービスなどが存在する。

システムによって、ハードウェアベンダーが異なるため、複数のメーカーのコンピュータが情報センター内に混在している。

インターネットとの接続ポイントには、ファイアウォールが設置されている。また、DMZ 上には、IDS が設置されている。ファイアウォールと IDS のログの確認には、外部のリアルタイム監視サービスを利用しており、外部から不正アクセスやウイルスの感染活動が発見された場合には、監視センターから連絡が来ることになっている。

.6.1 ＩＤＣセンターのサービス関連資産

関連サービス名	目的	仕様（機能）、製品名称	備考

共通	ファイアウォールによるアクセス制御（C）	専用ソフトによる SPI 方式のファイアウォール（Firewall-1）　4 セット	
共通	ファイアウォール	専用サーバ 4 台(Nokia 社)	
共通	F/W の LB（A）	LB 装置（Alteon 社 SeverIron）	
マネジメント	サーバ監視（I）	SNMP による監視・管理ソフトウェア エージェントソフトウエア （HP 社 OpenView）	
マネジメント	サーバ監視（I）	UNIX サーバ 2 台（HP 社） コールドスタンバイ	
マネジメント	アプリケーション稼動監視(I)	WWW サーバ稼動監視 Mercury SiteScope　4 セット	
マネジメント		Windows サーバ　4 セット	
共通	ドメイン名維持(I)	DNS サーバ Primary、SecondaryDNS の提供	
共通	ドメイン名維持	UNIX サーバ 2 台 （SunMicrosysytems 社）	
共通	Syslog 収集	UNIX サーバ 2 台	
マネジメント	バックアップ	SAN SANRISE H12000	
共通	ネットワークインフラ	ルータ　？台（Cisco 社）	
共通	ネットワークインフラ	L3SW,L2SW	
セキュリティ	不正パケット検出 IDS	専用装置（ISS 社 Proventia）2 セット	
セキュリティ	認証サーバ	LDAP Sun Directory Server　2 セット	
セキュリティ	認証サーバ	UNIX サーバ 2 台 （ SunMicrosysytems 社）	
セキュリティ	ワンタイムパスワード管理 RAS 認証サーバ	ACE/Server(RSA 社) ホスティングサービス向けコンテンツ修正	
セキュリティ	ワンタイムパスワード	RSA SecurID　トークン　?台	
ホスティング	Web ホスティング	ApacheWeb	
ホスティング	Web ホスティング	UNIX サーバ	
ホスティング	Web ホスティングの LB（A）	LB 装置（Alteon 社 SeverIron）	
セキュリティ	URL フィルタリング	InterSafe	
セキュリティ	URL フィルタリング	UNIX サーバ　2 台 （ SunMicrosysytems 社）	
セキュリティ	ウィルス対策プロキシサーバ	SMTP、HTTP サービス向けウィルスフィルタ TrendMicro 社製　InterScan　2 セット	
セキュリティ	ウィルス対策プロキシサーバ	UNIX サーバ　2 台 （ SunMicrosysytems 社）	
セキュリティ	ウィルス対策の LB（A）	LB 装置（Alteon 社 SeverIron）	

セキュリティ	証明書発行 CA	IIS Win2003Server	
セキュリティ	証明書発行 CA	Windows サーバ　2 台	
共通	ISP 回線	1Gb/s　2 回線	
共通	サーバラック	19inch ?台	

.6.2 ファシリティ関連資産

関連サービス名	目的	仕様（機能）、製品名称	備考
ファシリティ	受変電設備		
	変圧器・分電盤、配電盤	二重化	
	配電設備/入力分岐盤　他 負荷設備/制御盤・操作盤	二重化	
	非常用発電装置 燃料タンク	ガスタービン	
	原動機 発電機		
	直流電源装置	DC 電源供給	
	自動始動発電機盤		
	給油口ユニットボックス		
	入力変圧機盤・直流分岐盤・蓄電池		
	空調設備/空冷 パッケージエアコン		
	入退室管理 ITV 監視システム		
	建物周囲/建物外壁	センター	
	火災・消火設備	ハロゲン	
	認証システム	指紋、IC カード	

7 情報センターの物理的環境およびセキュリティ

.7.1 人的セキュリティ

(1)アクセス権限の識別

入退出に関する考え方は、以下の一般オフィス区画(1F／2F)と情報センター機能を持つ情報センター区画(3F～5F)に分けてその重要度に応じた入退出管理･監視機能を考慮する。

特に、情報センター区画へのアクセス制御は各エリア単位に独立性を確保する。

(2)入退出管理

上記のアクセス権限識別に設定された非接触型 IC カードにより、項番2の物理的セキュリティに示す、区画、エリアのドア開閉を非接触型 IC ｶｰﾄﾞにてコントロールする。

また、各ドアの両側に監視カメラを設置してある。

.7.2 物理的セキュリティ(建物要件)

1) 一般オフィス区画(1F～2F)

① 総合受付（午前８時から午後７時 30 分まで）・・・社内案内人＋外部委託警備会社警備員

② 夜間出入り口（午後７時以降午前８時まで）

夜間警備のため外部委託警備会社警備員が受付業務も行う。

③ 食堂（営業時間：午前１１時から午後１４時）・・・・1F

④ 来客用会議室・・・・１Ｆ

⑤ オフィス・・・・１Ｆ&2Ｆ

１Ｆ：営業部

２Ｆ：総務部、企画部、人事部

⑥ 機器及び情報センター関連機器及び媒体搬入口・・・・１Ｆ

機器搬入のための入り口であり人の出入りは禁止されている。

2) 情報センター区画 (3F～5F)

① 情報センター管理エリア・・・・３Ｆ

外部警備会社要員が２４時間常駐

a)センター受付・・・・3F

IDC センター常勤勤務者及び外来者（保守関連ベンダー等）の受け付け。特に外来者の場合は、事前申請書と本人確認できる物との照合により受け付け処理を行い、必要作業・行為に相当する臨時入館カードを付与する。

尚、夜間入館は 1F 夜間入り口より入館し、3F のセンター受付にて、IDC センター入館手続きとる。

(参考：情報センター入退出管理手引きに準じた運営)

b)ビル中央監視室(防災センター)・・・・3F

IDC センター全体建物設備(電源・空調等)を監視するためのエリア

② システム執務室・・・・3F

a)オペレータ控え室

２４時間３６５日システム稼働を実施するためにオペレータを２グループ体制として、引継ぎを受けるオペレータの控え室。

また、緊急時のオペレーション体制の場合の控え室。

b)オペレーション引継ぎ等会議スペース

c)各種ドキュメント・記録・申請書・契約書保管(キャビネット類)

③ オペレーションエリア・・・・3F

a)システムオペレーション室

システム稼働状況監視及びハンドリング作業エリア

④ 電算機室エリア・・・・4F

a) 各種サーバ設置区画

b) バッテリー室

c) UPS 室

⑤ 大量印刷エリア・・・・4F

レーザプリンター、インパクトプリンター、媒体変換機(ＣＤ－R 焼き付け等)を設置エリア

⑥ デリバリー関連エリア・・・・４Ｆ

ここに示す以下の各エリアはそれぞれ独立したエリアとして特に媒体等の受け渡しについては、確実に行えるようにドアの開閉制御を行う。具体的には、オペレーションを行った要員が直接デリバリー作業を行はないようにする。

a)用紙等媒体倉庫

印刷サービス用帳票用紙、CD－R 等の格納倉庫

b)カートリッジ・MT 倉庫

システム入出力用のカートリッジ・MT 等の保管場所(結露を考慮して温度調整されたエリア)。このエリアでの作業は行はない。

c)仕分け室

システム出力媒体(カートリッジ・印刷帳票等)の顧客別、発送先別に仕分けを行う作業エリア

ｄ）バックアップ媒体保管室・・・・4F

⑦ 電源・空調・通信等設備エリア・・・・ＢＦ１

a)発電機室

非常電源発電機設置室

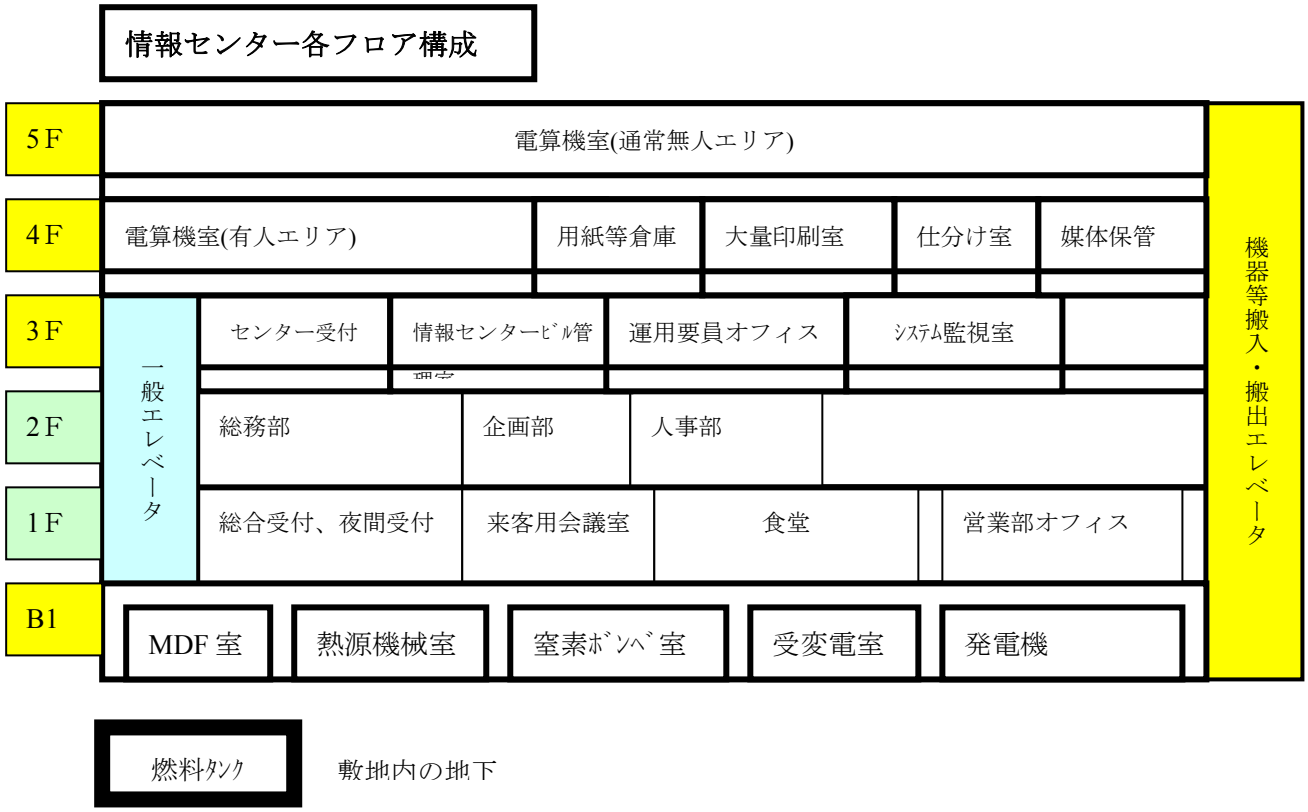
b)熱源機械室

c)受変電室

受電電源変圧機器設置

d)MDF 室

通信ケーブル集約室



.7.3 退出管理の基本方針

重要区画の管理方針は各従業員の業務権限に沿ったICカードによる本人認証を個別エリア入退出時に行う。

外部訪問者および情報センター区画への外部委託業者等の入出に際しては別途定める「情報センター利用規程」に沿って事前申請制をとり作業に応じたICカードを貸し出す。

(1)設備系(電源・空調・通信等設備エリア・・・BF1)

地下1階（BF1）に電源設備および外部送電取り入れ口、通信ケーブル受け口を設け厳重なる入退出管理エリアとする。一般オフィス区画とは分離されたエリアで(3)の情報センター区画と同等の管理

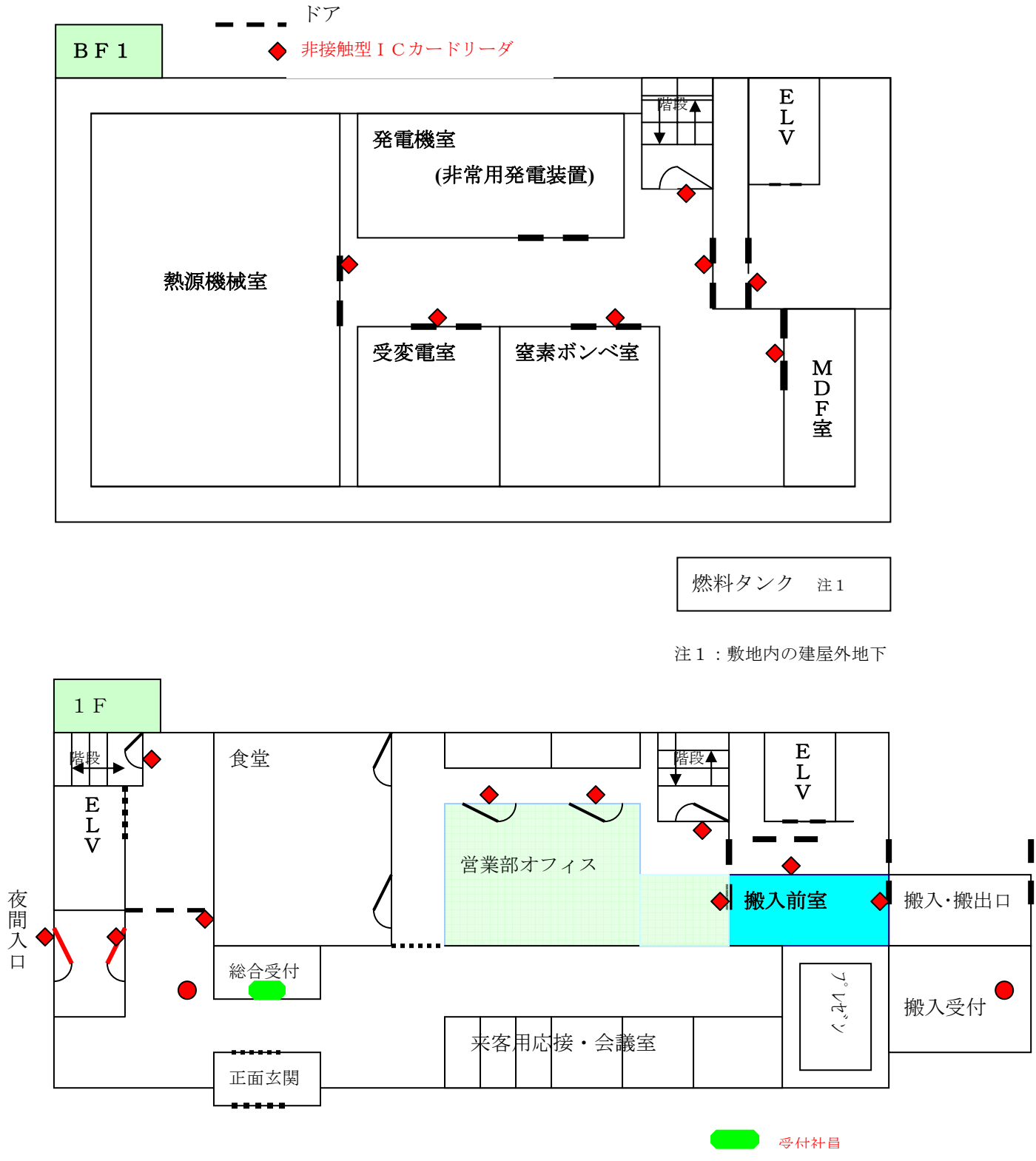
(2)一般オフィス区画（1F・2F）

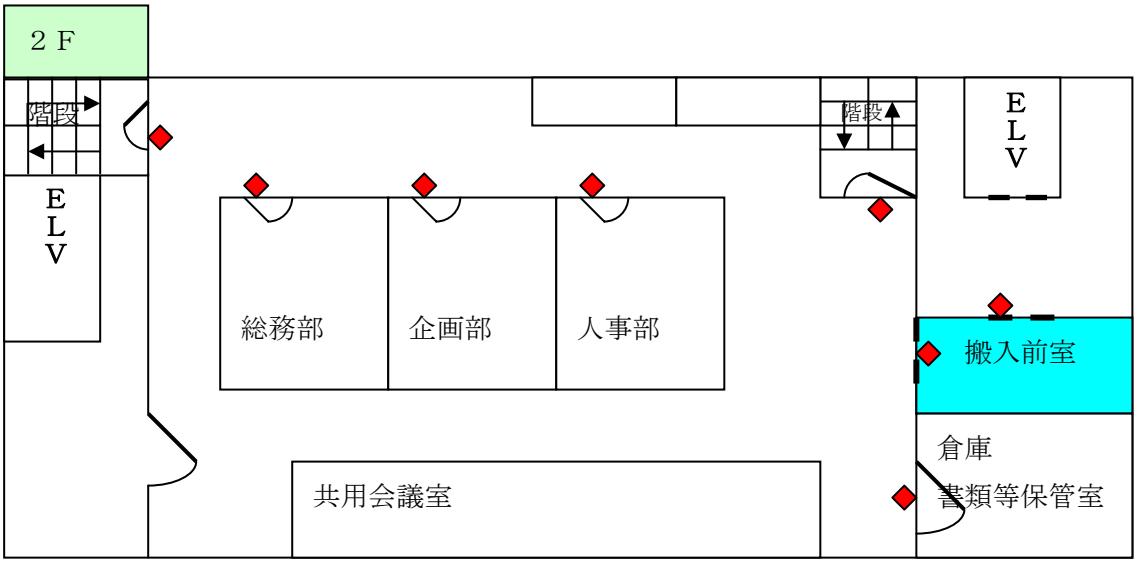
比較的自由度のある管理エリア

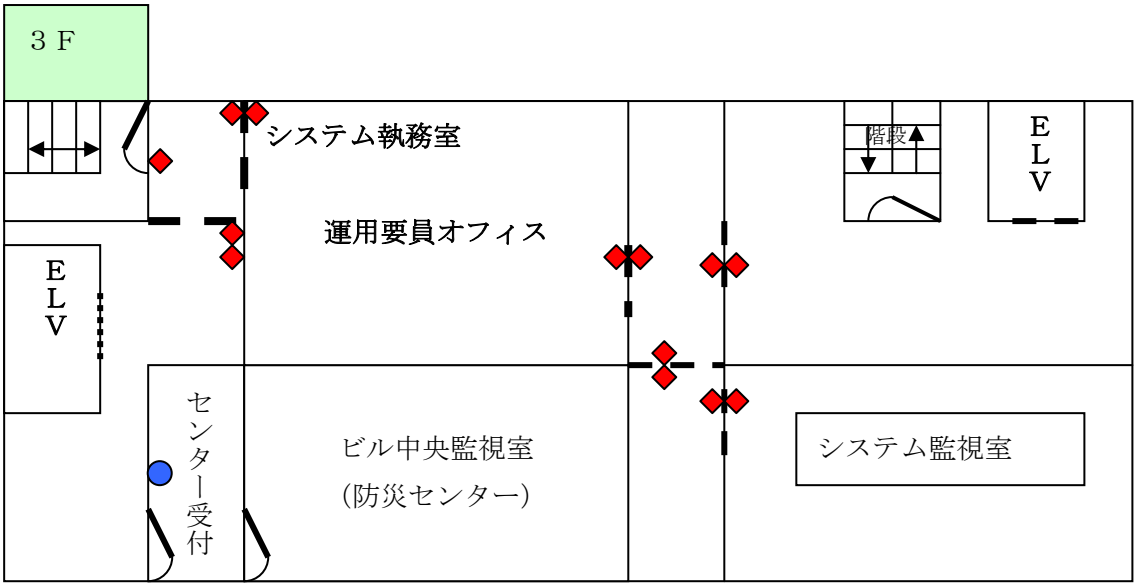
(3)情報センター区画(3F・4F・5F)

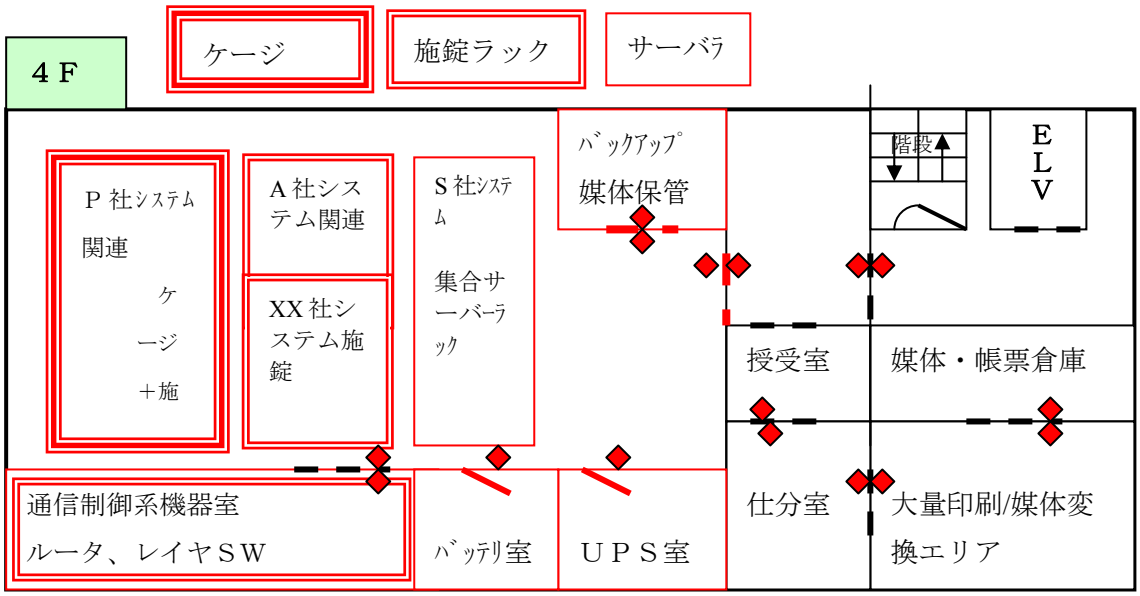
最重要管理

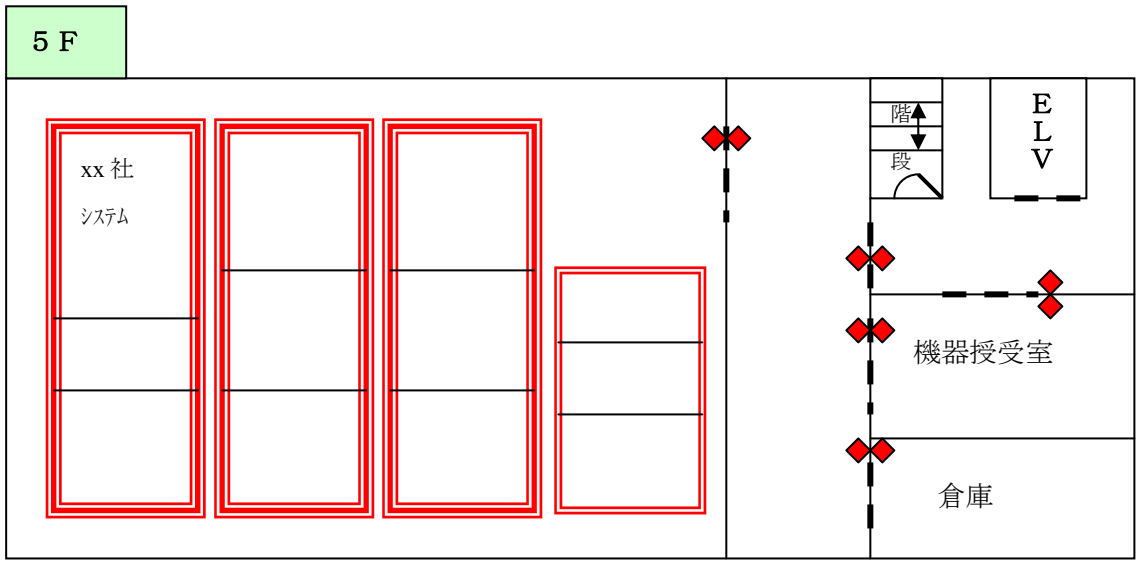
.7.4 情報センターレイアウト




２Ｆ
階段
ＥＬＶ
総務部
企画部
人事部
階段
ＥＬＶ
搬入前室
倉庫
書類等保管室
共用会議室


３Ｆ
システム執務室
運用要員オフィス
階段
ＥＬＶ
ＥＬＶ
センター受付
ビル中央監視室
(防災センター)
システム監視室





.7.5 開発・バックアップセンター

電算仕様の賃貸ビル（3フロア賃貸／ビル全体は5フロア）

機能：開発センター、バックアップデータ隔地保管

1) **人的セキュリティ**

各エリアは職務権限(アクセス権限)に応じた入退出用 IC カードによりドアの開閉制御を行う。

2) **物理的セキュリティ（賃貸2フロア：4・5F）**

他社との同居であるため S 社賃貸各フロアで物理的セキュリティの確保を要する。

①受付

②開発機・バックアップ機設置エリア

③開発作業エリア

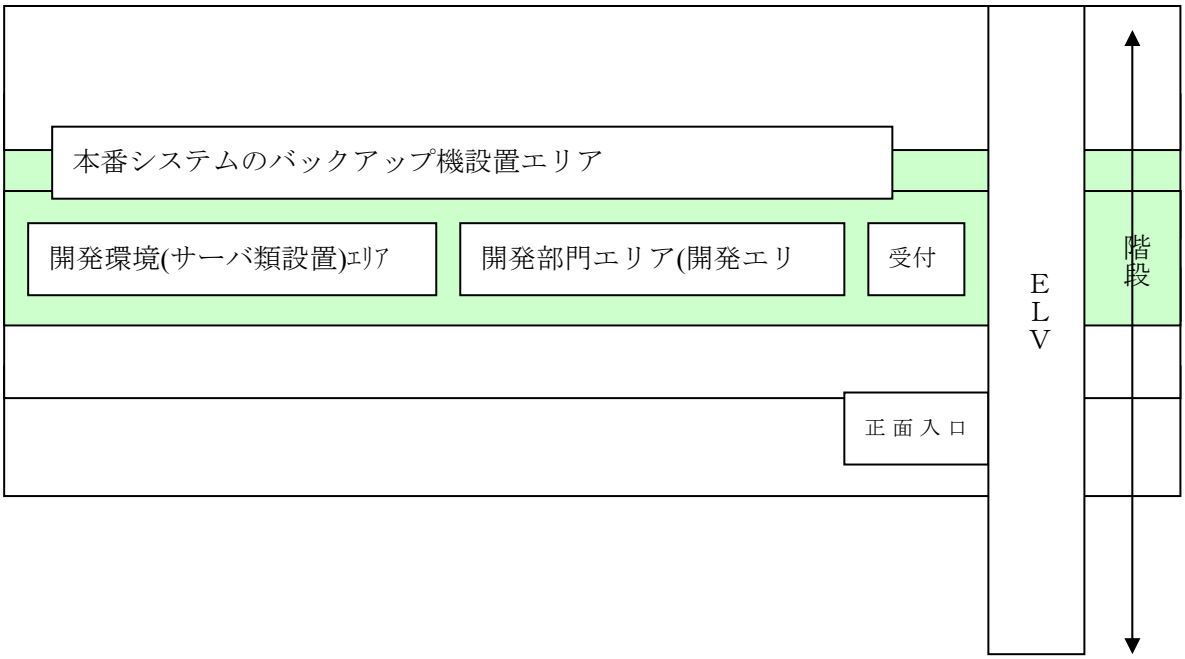
3) **開発作業フロア（開発ルーム）**

開発端末（クライアントPC），開発関連資料保管室（ドキュメント類、ドキュメント媒体）

開発機設置フロア

バックアップ機設置フロア

≪各フロア構成≫



8 データ

バックアップは、世代管理を行っている。重要システムのフルバックアップ・データの一部は、旧情報センターに定期的に送られている。

P社から預託を受けているデータの中には、個人情報に属する情報も含まれている。S社においても、単にバックアップを取る等の作業だけでなく、一部の個人データについては、内容を閲覧したり、変更したりする業務を受けている。

9 受託システム例

.9.1 データベース・システム

S 社は、グループ会社のA社から、ポイントカード・システムのデータベース・システムの運用を受託している。A社では、顧客にポイントカードを発行しているが、ポイントカード・システムのメンバーに対する特典の一つとして、ウェブサイトのポイントカード・メンバー・ページ上でさまざまな機能を提供している。メンバーは、ID とパスワードでメンバーページにアクセスする。アンケートに答えると一定の人数の回答者にポイントが当たるサービスや、メンバーページ上からキャンペーンに応募できるサービス、メンバーページ上から簡単に予約できるサービス、事前に登録しておいたジャンルの情報だけを表示するサービス、現在のポイント数を確認できるサービス、ポイントを景品に交換できるサービスなどがある。このため、ウェブサーバとデータベースサーバを連携させ、データベース上の各メンバー固有の情報にアクセスしている。

メンバーの情報を照会できるのは、A社の担当者と、委託先の S 社の担当者である。担当者は、リモートアクセス、または、オンサイトアクセスによって、メンバー情報の照会、閲覧、変更、消去などが可能である。

.9.2 海外業務システム

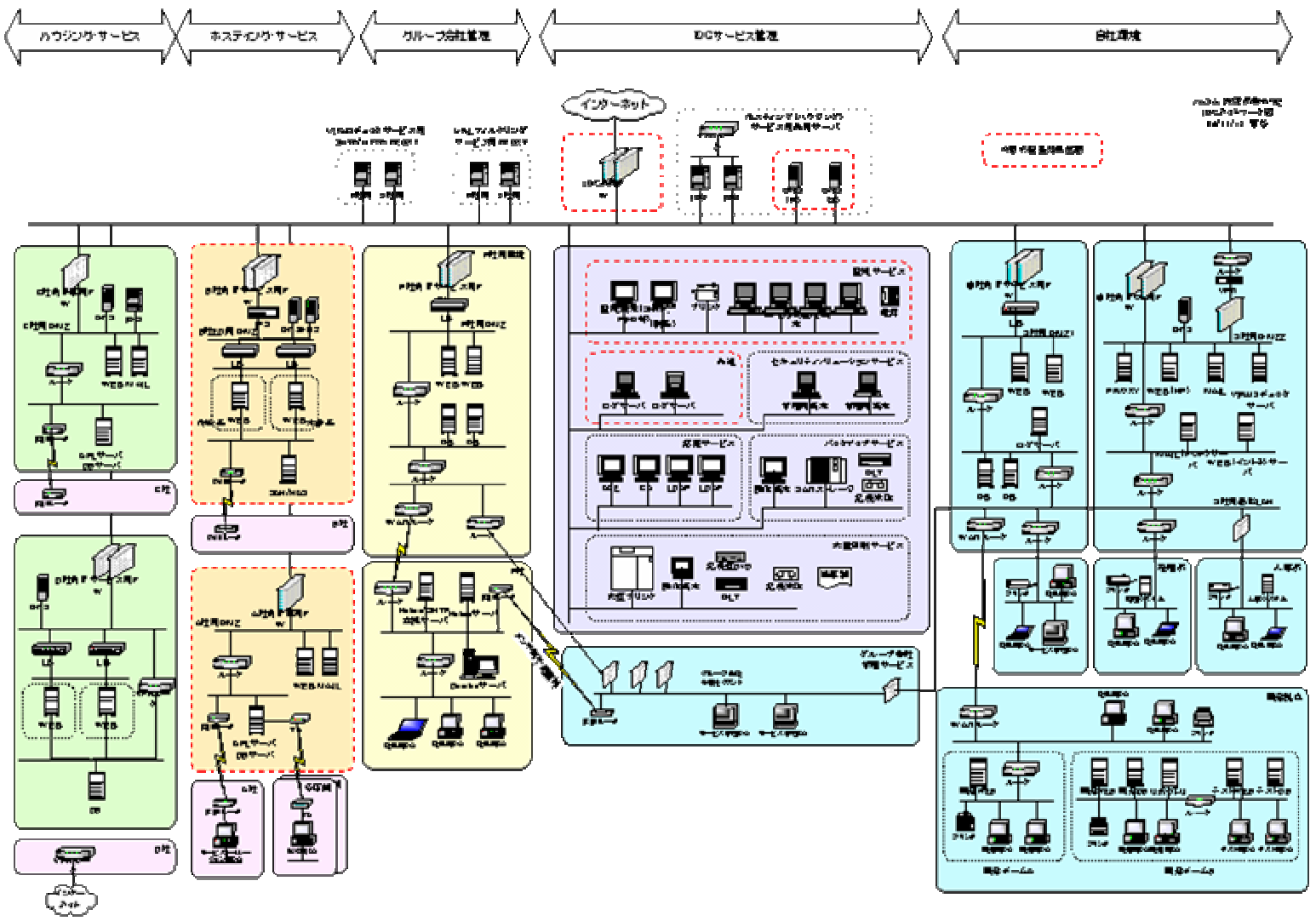
S 社は、グループ会社のB社から、海外の支店、顧客との間で、資材の取引を行う業務システムの運用を受託している。このシステムは、ウェブサーバで実現されており、海外の支店、顧客は、認証を受けた上でこのシステムにアクセスし、売買情報を入力する。売り主が余剰資材の情報、引き渡し条件、引き渡し価格を入力し、買い主は、買いたい資材があれば、希望購入価格や購入条件のオファーを出す。売り主は、オファーのタイミングや、希望条件を勘案して、取引成立であれば個別交渉に入る。大きな金額が動く商談であり、また、24 時間稼働が必要であるため、特にシステムの信頼性が求められている。S社は、B社から、障害の緊急対応などの運用業務を受託している。

.9.3 オンラインショッピングシステム

グループ会社の D 社は、S 社のハウジングサービスを利用して、オンラインショッピングシステムを稼働させている。D 社のオンラインショッピングサイトでは、小売店で販売している商品の一部と、オンラインショッピング専用の商品（プレミアムグッズ等）が購入可能である。ユーザーが、ブラウザで D 社のオンラインショッピングサイトにアクセスすると、商品カタログの閲覧と検索が可能である。いわゆるショッピングカート機能になっており、ユーザーは購入したい商品をショッピングカートに入れておき、商品の選択が完了すると、カードで決済する手順となる。カード決済機能は、カード会社のモジュールを利用しており、実際のカード決済の部分では、ウェブアプリケーションは、カード会社のシステムと通信を行い、サービスを完結する。氏名、クレジット番号、有効期限などの入力時には、SSL を利用した暗号通信を利用している。D 社では、購入結果に基づいて、購入された商品の発送を行っ

ている。また、商品未達、返品希望などの問い合わせ窓口を設けて、ユーザーからの問い合わせに応対している。

10　S社のネットワーク環境



11 Ｓ社の各サービスにおける情報資産

.11.1 マシンレンタル（ホスティング）サービス

大項目	中項目	小項目	備考
文書・データ	システム構成情報	ネットワーク構成図	IPアドレス等含む
		システム構成情報	
	システム設定情報	ネットワーク機器の設定情報	FW、ルータ、LB、TA、IPS等レンタル機器内の設定情報
		サーバ設定情報	DNS サーバ、WEBサーバ、メールサーバ、DBサーバ等レンタル機器内の設定情報
		アカウント情報	各種サーバのID、パスワード
	システム運用情報	システムログ（OSレベル）	SYSLOG、ログインログ（wtmp 等）
		システムログ（ミドルウェアレベル）	WEB サーバ（apache 等）、RDBMS のログ
		稼動ログ	ホスティング対象機器のシステム稼動監視ログ
	サービス関連情報	手順書類	自センター作成の障害対応手順書
		サービス報告書	運用報告書、作業記録、障害報告書
		契約書類	サービス申込書、顧客との契約、ベンダーとの契約、NDA等
	業務系記録	構成変更記録	
		作業記録	オペレータ日次処理、障害復旧作業処理
	顧客がオーナの情報	設計書類	要件定義書、概要設計書、詳細設計書
		手順書類	顧客側作成のシステム運用手順書、障害対応手順書
		プログラムソース	CGIプログラム、JAVA
		WEBコンテンツ	HTML
		テスト関連文書	テスト計画、結果報告書
		サービス関連データ	顧客が提供するサービスのデータ
		デジタル証明書	サーバ証明書
		電子メール	
ソフトウェア	レンタル対象ソフトウェア	各サーバOS	レンタルサーバ用
		ミドルウェア	WEB サーバ（apache 等）、MAILサーバ（sendmail 等）、DNSサーバ（bind 等）、RDBMS等
		ウィルス対策ソフト	レンタルサーバ用

	システムソフトウェア	各サーバOS	監視端末等用
	業務系ソフトウェア	操作記録取得ソフト	
		モニタリングソフト	SNMPエージェント、SNMPコンソール
ハードウェア	レンタル対象ハードウェア	ネットワーク機器	FW、ルータ、LB、TA、IPS等レンタル機器、ケーブル
		サーバ機器	DNS サーバ、WEBサーバ、メールサーバ、DBサーバ、ログサーバ等レンタル機器
	業務用ハードウェア	SNMP操作端末	
		APL稼動監視端末	
	記憶装置・媒体	記憶装置・媒体	CD－ROM等
	付帯設備	プリンタ	
		電話	

.11.2 接続サービス

大項目	中項目	小項目	備考
文書・データ	システム構成情報	ネットワーク構成図	IPアドレス等含む
		システム構成情報	
	システム設定情報	ネットワーク機器の設定情報	FW、ルータ、VPN 機器内の設定情報
		サーバ設定情報	接続サービス提供機器（DNS、MAIL サーバ）内の設定情報
		アカウント情報	各種サーバのID、パスワード
	システム運用情報	システムログ（OSレベル）	SYSLOG、ログインログ（wtmp 等）
		システムログ（ミドルウェアレベル）	FW のログ（accept/deny）
		稼動ログ	接続サービス提供機器のシステム稼動監視ログ
	サービス関連情報	手順書類	自センター作成の障害対応手順書
		サービス報告書	運用報告書、作業記録、障害報告書
		契約書類	サービス申込書、顧客との契約、ベンダーとの契約、NDA等
	業務系記録	構成変更記録	
		作業記録	オペレータ日次処理、障害復旧作業処理

ソフトウェア	システムソフトウェア	各サーバOS	監視端末等用
	業務系ソフトウェア	操作記録取得ソフト	
		モニタリングソフト	MAIL サーバ、DNS サーバ、SNMPエージェント、SNMPコンソール
ハードウェア	業務用ハードウェア	ネットワーク機器	FW、ルータ、LB、VPN 等機器、ケーブル
		サーバ機器	DNS サーバ、MAIL サーバ
		SNMP操作端末	
		APL稼動監視端末	
	回線	上位 ISP との接続回線	2回線
	付帯設備	プリンタ	
		電話	

.11.3 監視サービス

大項目	中項目	小項目	備考
文書・データ	システム構成情報	ネットワーク構成図	IPアドレス等含む
		システム構成情報	
	システム設定情報	サーバのコンフィグレーション	監視サーバの設定情報
		エージェントのコンフィグレーション	監視対象サーバに導入する監視エージェントの設定情報
		アカウント情報	各種サーバ、監視端末のID、パスワード
	システム運用情報	システムログ（OSレベル）	SYSLOG、ログインログ（wtmp 等）
		システムログ（ミドルウェアレベル）	FW のログ（accept/deny）
		稼動ログ	接続サービス提供機器のシステム稼動監視ログ
	サービス関連情報	サービス管理台帳	プロセス監視、ログ監視、リソース監視、アプリケーション監視、 パフォーマンス監視等の対象機器（顧客名、IPアドレス）と監視内容、アラート発生条件等の一覧
		連絡先リスト	緊急時連絡先のリスト
		手順書類	作業手順書、緊急時連絡手順書、障害対応手順書等

		サービス報告書	運用報告書、作業記録、障害報告書
		契約書類	サービス申込書、顧客との契約、ベンダーとの契約、NDA等
	業務系記録	構成変更記録	
		作業記録	オペレータ日次処理、障害復旧作業処理
		障害履歴	障害発生・報告の記録
ソフトウェア	システムソフトウェア	各サーバOS	監視端末等用
	業務系ソフトウェア	操作記録取得ソフト	
		モニタリングソフト	SNMPエージェント、SNMPコンソール
ハードウェア	業務用ハードウェア	サーバ機器	監視サーバ
		SNMP操作端末	
		APL稼動監視端末	
	付帯設備	バックアップ装置	
		バックアップメディア	
		連絡用電話	

.11.4 ファシリティ

大項目	中項目	小項目	備考
文書・データ	システム構成情報	入退認証システム設計書	
		ビル設計、鳥瞰図など	
	システム設定情報	入退認証システムのコンフィグレーション	
		入退室アクセス制御設定	
		入退室者登録情報（従業員、顧客）	
		アカウント情報	各種サーバ、クライアントのID、パスワード
	システム運用情報	入退認証システムのログ	SYSLOG、ログインログ（wtmp 等）
	サービス関連情報	契約書類	サービス申込書、顧客との契約、ベンダーとの契約、NDA等
		手順書類	センタ管理システムの運用手順書、障害対応手順書等

	業務系記録	入退出ログ	入退認証システムによる入退出ログ
		監視映像	監視ビデオカメラによる映像記録
		入退認証システム作業／変更履歴	
		入館申請書、IC カード作成申請書	
		ラック鍵貸出簿	
ソフトウェア	システムソフトウェア	各サーバOS	
	業務系ソフトウェア	入退認証ソフト	
ハードウェア	サーバ	入退認証サーバ	
	クライアント	入退認証オペレータ端末	
	付帯設備<< 入退出関連 >>	建物周囲/建物外壁	センター建屋、受付、ビル中央監視室、B1F、サーバ室など
		IC カード	
		IC カードリーダ、ライタ	IC カード作成装置および各扉横に設置するカードリーダ
		監視カメラ、映像記録装置	
		ラックおよびラック鍵	
	付帯設備 << 電源、空調、通信 >>	受変電設備/配電設備/入力分岐盤　他負荷設備/制御盤・操作盤	二重化
		変圧器・分電盤、配電盤	二重化
		入力変圧機盤・直流分岐盤・蓄電池、UPS	
		電源ケーブル	
		通信ケーブル	
		直流電源装置	DC 電源供給
		自動始動発電機盤（非常用発電装置）	
		非常用発電装置　燃料タンク	ガスタービン
		給油口ユニットボックス	
		空調設備/空冷パッケージエアコン	
		窒素ボンベ設備	
		火災・消火設備	ハロゲン

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
5.2	装置のセキュリティ	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	1) 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること	1) 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること	7.2.1	○	マシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）装置及び通信機器はラックなどに収納し、施錠を行うこと。	ここでは、各サービスにおける次の装置等を想定する。
				2) 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること	7.2.1	○	マシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）装置及び通信機器のコンソール画面にはフィルタを設置し、視認できる範囲を限定すること。 コンソール画面はラック内に設置し、作業中も周囲の目からできる限り制限すること。	・マシンレンタルサービス：レンタル用サーバおよび通信機器。
				3) 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること	7.2.1	○	マシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）で利用する個人情報、パスワード情報が格納された場合には、高いレベルに分類し区画を分離して設置すること。	・接続サービス：インターネット接続に必要な、FWサーバおよびルータ等の通信機器。
				4) 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の策定を考慮すること	7.2.1	×		・監視サービス：監視用の端末等
				5) 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること	7.2.1	○	マシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）装置及び通信機器を設置するマシンルーム内あるいは、ラック内について、温度、湿度を測定する機器を設置し、室温上昇などによる機器の損傷がないか監視すること。	・ファシリティ：入退館管理装置、監視カメラ等
				6) 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること	7.2.1	○	マシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）装置及び通信機器のキーボード、電源スイッチ、モード切替のボタン等には、誤って、不用意な操作が行わないようカバー等で保護すること。 機器はラックに設置し、周囲を通過する際の接触等による損傷から防護を行うこと。	
				7) 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること	7.2.1	×		
			2) 装置は、停電、その他の電源異常から保護すること	1) 装置は、装置製造者の仕様に適合した適切な電力の供給を確保すること	7.2.2	×		
				2) 電源の多重化をすること	7.2.2	×		
				3) 無停電電源装置（UPS）を設置する	7.2.2	×		
				4) 非常用発電機の設置をすること	7.2.2	×		
				5) 障害対策計画では、UPSが故障した場合に取るべき措置についても計画しておくこと	7.2.2	×		
				6) UPSは、容量が十分であることを定期的に確認すること	7.2.2	×		
				7) UPSは、製造者の推奨に従って点検すること	7.2.2	×		
				8) 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること	7.2.2	×		
				9) 発電機を使用する場合、製造者の推奨に従って定期的に点検すること	7.2.2	×		
				10) 発電機を長時間運転できるように、燃料の十分な供給を確保すること	7.2.2	×		
				11) 電源の緊急スイッチは、機械室の非常口近くに設置すること	7.2.2	×		
				12) 主電源の停電時用として非常用照明を備えること	7.2.2	×		
				13) 落雷防護はすべての建物に備えること	7.2.2	×		
				14) すべての外部通信回線に落雷防護フィルタを付けること	7.2.2	×		
			3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受	1) 情報処理設備に接続する電源ケーブル及び通信回線は、可能ならば地下に埋設するか、又はそれに代わる十分な保護手段を施すこと	7.2.3	×		
				2) ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること	7.2.3	○	マシンレンタル用のサーバ装置及び通信機器とネットワークケーブルの接続は容易に損傷、変更できないように保護すること。 方法としては、床下、専用管、天井裏への配線を用いて、不用意な接触、認可されていない者の操作を防ぎ、電磁波漏れが懸念される場合は防磁用のケーブル、管を採用すること。	ネットワークケーブルに関する管理は、各サービスに付随するハードウェアの一部として、各サービス毎に掘り下げる。
				3) 干渉を防止するために、電源ケーブルは通信ケーブルから隔離すること	7.2.3	○	マシンレンタル用のサーバ装置及び通信機器を設置したラック内の配線は電源と通信のケーブルを離すか、シールドなどの保護を行うこと。	
				4) 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること	7.2.3	○	ユーザ情報や機密レベルの高い情報を保有するマシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）装置は他のサーバのケーブルとは別に外装電線管などを用いて損傷などから保護すること。	
				5) 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること	7.2.3	○	マシンレンタル用のサーバ装置及び通信機器で、通信ケーブルの接続部分などは修正が行われないようカバーなどを付けて施錠、封印を行うこと。	
				6) 取扱いに慎重を要するシステム又は重要なシステムに対しては、代替経路又は伝送媒体を使用すること	7.2.3	○	マシンレンタル用のサーバ装置及び通信機器の重要なデータ授受には経路上での漏洩を防ぐ為、外部記憶媒体を使用するか、公開用のネットワークとは別に保護された配線を行うこと。	
				7) 取扱に慎重を要するシステム又は重要なシステムに対しては、光ファイバケーブルを使用すること	7.2.3	○	マシンレンタル用のサーバ装置で、機密性の高い個人情報などが暗号化されず送信される場合には電磁波傍受などの脅威を防ぐ必要がある場合、対策として光ファイバーを用いること。	
				8) 認可されていない装置がケーブルに取り付けられているかどうかについての調査すること	7.2.3	○	マシンレンタル用のサーバ装置を接続する通信機器スイッチなどの接続ポートで使用していないものは無効設定とするか、封印を行い使用されていないか定期的に確認する。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく	1) 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること	7.2.4	○	マシンレンタル用のサーバ装置及び通信機器は、仕様書等であらかじめ定められた整備間隔に基づき定められた保守作業を実施すること。	
				2) 認可された保守担当者だけが装置の修理及び手入れを実施すること	7.2.4	○	マシンレンタル用のサーバ装置及び通信機器は、保守契約先からの担当者のみ、あるいは認可された担当者のみとし、 作業時には、サーバ管理者、サーバ管理者に権限を委譲	
				3) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること	7.2.4	○	マシンレンタル用のサーバ装置及び通信機器の保守作業中の内容について全てのコマンドなどの記録を行う機能を有すること。装置の保守内容を検証し、予防措置に努めること。	
				4) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること	7.2.4	○	マシンレンタル用のサーバ装置及び通信機器のシステムログに障害に関する情報が記録されていること。 この障害時の保守記録について対応記録をサーバ設置場所とは別に、保管されていること。	
				5) 装置を保守するために搬出する場合、適切な管理策を施すこと	7.2.4	○	マシンレンタル用のサーバ装置及び通信機器の搬出時にはデータのバックアップを実施後、消磁器の利用を実施、確認されていること。	
				6) 保険約款によって定められたすべての要求事項に従うこと	7.2.4	×		
			5) 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可	1) 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること	7.2.5	×		接続サービス、監視サービスにおいて、専門家が自宅よりリモート接続して操作することを想定している。
				2) 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと	7.2.5	×		
				3) ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること	7.2.5	×		
				4) 装置の保護に関しては、製造者の指示に常に従うこと	7.2.5	×		
				5) 在宅作業についての管理策は、リスクアセスメントによって決定するこ	7.2.5	×		
				6) 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること	7.2.5	×		
				7) 事業所外の装置を保護するために、十分な保険が付保されているこ	7.2.5	×		
				8) セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること	7.2.5	×		
			6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること	1) 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること	7.2.6	○	マシンレンタル用のサーバ装置及び通信機器で使用されたディスクの廃棄やサーバ障害などで交換されたディスクは読み取り不可能な状態にすること。 分解、破砕を行う。 困難な場合、データの上書きを行う、消磁器を用いた後、データの残留検査を実施すること。、	ファシリティでは、生態認証の情報等を想定している。
				2) 取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアが、消去又は上書きされているか確認すること	7.2.6	○	マシンレンタル用のサーバ装置及び通信機器で取り扱いに慎重を要するサーバの設定情報やアカウントの情報など、機密性を重要とされるデータは消去、別のデータの上書きを実施していること。	
5.3	その他の管理策	情報及び情報処理設備の損傷又は盗難を防止するため	1) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用 並びに情報処理設	1) クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること	7.3.1	×		
				2) クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること	7.3.1	×		
				3) 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管す	7.3.1	×		
				4) 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと	7.3.1	×		
				5) パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと	7.3.1	×		
				6) パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること	7.3.1	×		
				7) 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること	7.3.1	×		
				8) 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと	7.3.1	×		
				9) 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと	7.3.1	×		
			2) 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできな	1) 持出し時及び返却時に記録を残すこと	7.3.2	×		
				2) 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること	7.3.2	×		
				3) 現場検査があることを各人が認識していること	7.3.2	×		
6.1	運用手順及び責任	情報処理設備の正確、かつ、セキュリティを保った運用を確実にす	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持し	1) 操作手順は、正式な文書として取り扱うこと	8.1.1	×		ファシリティでは、入退室管理、各種制御系システムを想定。
				2) 操作手順が変更の場合は管理者によって認可されること	8.1.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 操作手順には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				4) 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				5) 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記	8.1.1	×		
				6) 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				7) 操作手順には、特別な出力の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記す	8.1.1	×		
				8) 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				9) 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること	8.1.1	×		
			2) 情報処理設備及びシステムの変更について管理すること	1) 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること	8.1.2	×		
				2) 運用プログラムは、厳重な変更管理の下に置くこと	8.1.2	○	マシンレンタル用のサーバ装置及び通信機器でのバックアッププログラム、コンテンツ管理システムの変更管理権限は厳重に管理し、作業施行記録を残すこと。	
				3) プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること	8.1.2	○	マシンレンタル用のサーバ置の監査記録は改ざんなどを行われないようにするため別のサーバへの転送、ハッシュをとるなどの処理を行うこと。	
				4) 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合すること	8.1.2	×		
				5) 重要な変更を識別及び記録すること	8.1.2	○	マシンレンタル用のサーバ装置の運用ユーティリティプログラム(ログ集計、コンテンツ管理、DBMS、メール）の改ざんチェック、あるいはハッシュを保管し監査記録を行うこと。	
				6) 重要な変更の潜在的な影響の評価をすること	8.1.2	×		
				7) 変更の申出を正式に承認する手順を確立すること	8.1.2	×		
				8) 変更の詳細の、全関係者への通知をすること	8.1.2	×		
				9) うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること	8.1.2	×		
			3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理	1) 情報システムの故障及びサービスの停止に対処できるように、手順を定めること	8.1.3	×		
				2) サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること	8.1.3	×		
				3) 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること	8.1.3	×		
				4) 機密性に対する違反に対処できるように、手順を定めること	8.1.3	×		
				5) 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を	8.1.3	×		
				6) 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること	8.1.3	×		
				7) 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること	8.1.3	×		
				8) 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること	8.1.3	×		
				9) 通常の障害対策計画手順には、監督機関に対する措置の報告を含め	8.1.3	×		
				10) 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	マシンレンタル用のサーバ装置及び通信機器でログの書込み権限は制限すること。 ログは2箇所以上に記録を実施し、実行IDや時間を記録し、改ざん等の発見を行うこと。 電子署名等による改ざん防止の対策を実施すること。	
				11) 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での証拠として使用するために、監査証跡及びこれに類	8.1.3	○	マシンレンタル用のサーバ置及び通信機器でログの書込み権限は制限すること。 ログは2箇所以上に記録を実施し、改ざん等の発見を行うこと。 電子署名等による改ざん防止の対策を実施すること。	
				12) ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	マシンレンタル用のアプリケーションサーバのログに関する設定などを行い、ログ収集を行うこと。 ログは2箇所以上に記録を実施し、改ざん等の発見を行うこと。	
				13) セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理さ	8.1.3	×		
				14) 事件・事故管理手順では、身分が明らかで、認可された要員だけに、作動中のシステム及びデータに対するアクセスを、許すことを考慮す	8.1.3	×		
				15) 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること	8.1.3	×		
				16) 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること	8.1.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				17) 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認することを考慮すること	8.1.3	×		
			4) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又	1) 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による監督といった他の管理策を考慮すること	8.1.4	×		
				2) セキュリティ監査は、独立性を維持すること	8.1.4	×		
				3) どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること	8.1.4	×		
				4) ある作業を始めることと、その作業を認可することとを分離すること	8.1.4	×		
				5) 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること	8.1.4	×		
				6) 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること	8.1.4	×		
			5) 開発施設、試験施設及び運用施設を分離するため、ソフトウェアの開発から運用の段階への移行についての規則を明	1) 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること	8.1.5	×		
				2) 同様な分離は、開発と試験との機能間でも実行すること	8.1.5	×		
				3) 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持す	8.1.5	×		
				4) 開発施設、試験施設及び運用施設を分離すること	8.1.5	○	マシンレンタル用のWebサーバのコンテンツ確認用サーバと公開用のサーバは区画を分けて不用意なアクセスを防ぐこと。 マシンレンタル用サーバの試験用のサーバと公開用のサーバは別区域として管理すること。	
				5) 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること	8.1.5	○	試験に持ちいる確認用サーバと、公開用のサーバは可能であれば別の機器とし、同一の機器であっても、ディスクパーティション、ディレクトリを分離し、利用権限は別にすること。	
				6) 開発作業と試験作業とは、可能な限り分離すること	8.1.5	○	マシンレンタル用サーバアプリケーションの試験作業はテストアプリケーションと本運用アプリケーションの誤用を避けるため、開発（変更）作業とは別室、別のサーバにて行うこと。	
				7) コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと	8.1.5	○	マシンレンタル用のサーバ（Web、DNS、SMTP、DB利用）で不要な開発用のツールは削除すること。 テキストエディタなどの運用作業上削除できないユーティリティは認可されたユーザのみ利用できる設定とすること。	
				8) 運用システム及び試験システムに対しては、異なるログオン手順を用いること	8.1.5	○	運用システムにログインするユーザIDは、コンテンツ確認用サーバとは別のユーザとすることで、公開用サーバと試験サーバを誤って操作することを防いでいること。	
				9) 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること	8.1.5	○	マシンレンタル用のサーバは公開サーバと試験サーバでは、パスワードは同一のものとしていないこと。	
				10) メニューには、適切な識別メッセージを表示すること	8.1.5	○	マシンレンタル用のサーバのメニューには試験用サーバと公開サーバの操作誤りを防ぐ為、メニューの色、ラベル、ウィンドウにメッセージなどを表示し、違いがわかるようなテンプレートを作成、表示すること。	
				11) 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得すること	8.1.5	○	マシンレンタル用のサーバにおいて、開発担当者がソフトウェアの不具合のため公開用サーバで作業を行う場合のIDが、システムの設定を変更できる管理者権限のIDではないこと。	
				12) 管理用パスワードは、使用後には変更されることを確実にすること	8.1.5	○	マシンレンタル用のサーバで開発担当者がソフトウェアの不具合のため公開用サーバで作業を行う場合、作業者が作業を実施した後にパスワード変更が行われ、作業時のパスワードで使用できないことを確認すること。	
			6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意	1) 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること	8.1.6	×		
				2) 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること	8.1.6	×		
				3) 外部委託による施設管理においては、事業継続計画との関連性を考	8.1.6	×		
				4) 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮する	8.1.6	×		
				5) 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当	8.1.6	×		
				6) 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順	8.1.6	×		
6.2	システムの計画作成及び受入れ	システム故障のリスクを最小限に抑えるため	1) 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること	1) 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること	8.2.1	○	コンテンツの急激な増加などに備え、資源管理の一環としてユーザごとの容量制限を実施すること。 メモリ使用状況など、SNMP監視機能を利用して情報を取得し、情報から統計情報を作成する手順、あるいはシステムを有すること。	・接続サービス：ネットワークトラフィック ・監視サービス：取得するログのディスク容量 等をそれぞれ想定している。

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資源の使用を監視すること	8.2.1	○	(該当しない) 汎用コンピュータは対象システム上に存在しない	
				3) 管理者は、使用傾向、特に業務用ソフトウェア又は情報システムの管理ツールと関連した傾向を識別すること	8.2.1	○	(該当しない) 汎用コンピュータは対象システム上に存在しない	
				4) システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を	8.2.1	○	(該当しない) 汎用コンピュータは対象システム上に存在しない	
			2) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受	1) 管理者は、新しいシステムを受け入れるための要求事項及び基準を明確に定義すること	8.2.2	×		
				2) 管理者は、新しいシステムを受け入れるための要求事項及び基準を文書化すること	8.2.2	×		
				3) 管理者は、新しいシステムを受け入れるための要求事項及び基準を合意すること	8.2.2	×		
				4) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な評価を実施する	8.2.2	×		
				5) 管理者は、新しいシステムを受け入れるための要求事項及び基準を、評価することを確実にすること	8.2.2	×		
				6) システムの受け入れにおいて、性能及びコンピュータの容量・能力の要求事項を考慮すること	8.2.2	×		
				7) システムの受け入れにおいて、誤りからの回復及び再起動の手順並びに障害対策計画を考慮すること	8.2.2	×		
				8) システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮するこ	8.2.2	×		
				9) システムの受け入れにおいて、合意された適切なセキュリティ管理策を考慮すること	8.2.2	×		
				10) システムの受け入れにおいて、手動による有効な手順を考慮すること	8.2.2	×		
				11) システムの受け入れにおいて、事業継続の取決めを考慮すること	8.2.2	×		
				12) システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること	8.2.2	×		
				13) システムの受け入れにおいて、新しいシステムが組織のセキュリティ全般に及ぼす影響について、検討したという証拠を得ること	8.2.2	×		
				14) システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと	8.2.2	×		
				15) 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと	8.2.2	×		
				16) 主要な新しいシステム開発においては、適切な試験を実施し、すべての受入れ基準が完全に満たされていることを確認すること	8.2.2	×		
6.3	悪意のあるソフトウェアからの保護	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	1) 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと	8.3.1	×		ウィルスについては、原則として、ウィルスチェックサービスの対象範囲とし、今回抽出したサービスでは個別に扱わない。ただし、監視サービスについては、監視用端末自体のウィルスチェックを想定したため、範囲に含んでいる。
				2) ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること	8.3.1	×		
				3) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクから保護し、どのような保護対策を行うことが望ましいかを示す組織としての個別方針を考慮すること	8.3.1	×		
				4) 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期	8.3.1	×		
				5) 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること	8.3.1	×		
				6) 未承認のファイル又は無認可の変更の存在に対しては、正式に調査	8.3.1	×		
				7) 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること	8.3.1	×		
				8) 電子メールの添付ファイル及びダウンロードしたファイルのすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること	8.3.1	×		
				9) システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること	8.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				10) ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考	8.3.1	×		
				11) ウイルス感染からの回復のための適切な事業継続計画を考慮するこ	8.3.1	×		
				12) 悪意のあるソフトウェアに関するすべての情報を確認すること	8.3.1	×		
				13) 警告情報が正確、かつ、役立つことを確実にするための手順を考慮す	8.3.1	×		
				14) 管理者は、単なるいたずらと真のウイルスとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること	8.3.1	×		
				15) 職員は、単なるいたずらの問題及びそれらを受け取ったときの対応について認識していること	8.3.1	×		
6.4	システムの維持管理 (Housekeeping)	情報処理及び通信サービスの完全性及び可用性を維持するため	1) 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること	1) 災害又は媒体故障が発生した後、極めて重要なすべての業務情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備えること	8.4.1	×		マシンレンタルサービスのバックアップは、レンタル先のクライアントが原則担当すうため、対象外とする。
				2) 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた	8.4.1	×		
				3) 重要な業務用ソフトウェアについては、少なくとも3世代又は3サイクル分のバックアップのための情報を保	8.4.1	×		
				4) バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施す	8.4.1	×		
				5) 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること	8.4.1	×		
				6) 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定し	8.4.1	×		
				7) バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること	8.4.1	×		
				8) 復元手順は、定期的に検査及び試験すること	8.4.1	×		
			2) 運用担当者は、自分の作業の記録を継続すること	1) 記録には、システムの起動及び終了の時刻を含めること	8.4.1	×		
				2) 記録には、システム誤り及び実施した是正処置を含めること	8.4.2	×		
				3) 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること	8.4.2	×		
				4) 記録には、記録の作成者の名前を含めること	8.4.2	×		
			3) 運用担当者の記録は、定期的に独立した検査を受けること	（なし）	8.4.2	×		
			4) 障害については報告を行い、是正処置をとること	1) 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること	8.4.3	×		
				2) 報告された障害の取扱いについては、明確な規定があること	8.4.3	×		
				3) 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと	8.4.3	×		
				4) 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを	8.4.3	×		
6.5	ネットワークの管理	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること	1) ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること	8.5.1	○	マシンレンタル用のサーバが他のサービスとネットワークを共有する場合には、別サービスからデータのモニタリングが不可能な環境とすること。	接続サービスについては、外部および内部のネットワークを想定、また、監視サービスについては、内部ネットワークを想定。
				2) ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること	8.5.1	○	マシンレンタル用のサーバへのアクセスはFirewall等によりサービスを制限する、認証機能を追加することで、無認可のアクセスから保護すること。	
				3) ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること	8.5.1	○	マシンレンタル用のサーバ管理者とネットワーク運用の責任者は可能であれば分離すること。	
				4) 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立す	8.5.1	×		
				5) 公衆ネットワークを通過するデータの機密性及び完全性を保護するため、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理策を確立すること	8.5.1	○	マシンレンタル用のサーバと利用者の経路の保護を行う場合、Webサーバ ではSSLを用いる、メンテナンスには専用の経路を設ける、SSH等を利用するといった、暗号化と認証を考慮すること。	
				6) サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整すること	8.5.1	○	マシンレンタル用のサーバと、Firewallのルール、ルータ間のルール、アプリケーションで利用するサービスの設定内容は矛盾がないよう調整を行うこと。	
6.6	媒体の取扱い及びセキュリティ	財産に対する損害及び事業活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること	1) 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること	8.6.1	×		
				2) 組織の管理外となる媒体のすべてについて、認可を必要とすること	8.6.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				3) 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること	8.6.1	×		
				4) すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること	8.6.1	×		
				5) コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書	8.6.1	×		
			2) 媒体が不要となった場合は、安全、かつ、確実に	1) 媒体の安全な処分のための、正式な手順を確立すること	8.6.1	×		
				2) 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること	8.6.2	×		
				3) 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること	8.6.2	×		
				4) 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと	8.6.2	×		
				5) 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること	8.6.2	×		
				6) 処分しようとする媒体を集める場合、集積することによる影響に配慮	8.6.2	×		
			3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	1) 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類	8.6.3	×		
				2) 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること	8.6.3	×		
				3) 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮	8.6.3	×		
				4) 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持につい	8.6.3	×		
				5) 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを	8.6.3	×		
				6) 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること	8.6.3	×		
				7) 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮す	8.6.3	×		
				8) 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること	8.6.3	×		
				9) 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて	8.6.3	×		
				10) 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること	8.6.3	×		
			4) 認可されていないアクセスからシステムに関する文書を保護すること	1) システムに関する文書は、安全に保管すること	8.6.4	×		
				2) システムに関する文書にアクセスできる者は、人数を最小限に抑えるこ	8.6.4	×		
				3) システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること	8.6.4	×		
				4) システムに関する文書で、公衆ネットワークの公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること	8.6.4	×		
6.7	情報及びソフトウェアの交換	組織間で交換される情報の紛失、改ざん又は誤用を防止するため	1) 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと	1) 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること	8.7.1	×		
				2) セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること	8.7.1	×		
				3) セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること	8.7.1	×		
				4) セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術基準標準を考慮するこ	8.7.1	×		
				5) セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること	8.7.1	×		
				6) セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること	8.7.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				7) セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考	8.7.1	×		
				8) セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考	8.7.1	×		
				9) セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考慮すること	8.7.1	○	Webコンテンツの授受やアクセスログの統計データなどは標準に従って行うこと。（例：CD-Rへの記録などはISOXXXXの規格） ファイルの形式は交換者間で合意されたフォーマットに準拠したソフトウェアなどを利用すること。 必要に応じ、パスワード、技術的に安全な暗号化を行うこと	
				10) セキュリティ条件にかかわる合意では、取扱いに慎重を要するもの（例えば、暗号かぎ）を保護するために必要とされる特別な管理策を考慮	8.7.1	×		
			2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること	1) 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること	8.7.2	×		
				2) 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いるこ	8.7.2	×		
				3) 媒体の配送においては、宅配業者の身分を確認する手順を導入する	8.7.2	×		
				4) 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること	8.7.2	×		
				5) 媒体の配送においては、施錠されたコンテナの使用を考慮すること	8.7.2	×		
				6) 媒体の配送においては、手渡しを考慮すること	8.7.2	×		
				7) 媒体の配送においては、開封防止包装の利用を考慮すること	8.7.2	×		
				8) 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること	8.7.2	×		
				9) 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること	8.7.2	×		
			3) 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること	1) 電子商取引のセキュリティにおいては、認証（買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求す	8.7.3	×		
				2) 電子商取引のセキュリティにおいては、認可（価格を決める権限、重要な取引文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか、取引相手はこれらをどう	8.7.3	×		
				3) 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること	8.7.3	×		
				4) 電子商取引のセキュリティにおいては、価格情報について考慮すること	8.7.3	×		
				5) 電子商取引のセキュリティにおいては、注文取引について考慮すること	8.7.3	×		
				6) 電子商取引のセキュリティにおいては、審査について考慮すること	8.7.3	×		
				7) 電子商取引のセキュリティにおいては、決済について考慮すること	8.7.3	×		
				8) 電子商取引のセキュリティにおいては、注文について考慮すること	8.7.3	×		
				9) 電子商取引のセキュリティにおいては、責任について考慮すること	8.7.3	×		
				10) 電子商取引に関する当事者間の合意は、権限の詳細も含め、合意した取引条件を両当事者に義務付ける契約書によって裏付けること	8.7.3	×		
				11) 情報サービス事業者と付加価値ネットワーク事業者との間にも、合意を交わすこと	8.7.3	×		
				12) 公開している取引システムでは、その取引条件を顧客に公表すること	8.7.3	×		
				13) 電子商取引に用いる基幹コンピュータのもつ攻撃に対する耐性について、及び電子商取引の実施に必要なネットワーク相互接続のセキュリティ上のかかわりについて、	8.7.3	×		
			4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること	1) 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること	8.7.4.1	○	マシンレンタル用のサーバでSMTPサーバを構築する際には以下の対策が可能な環境、ユーザによって実施されていることについて考慮すること。 （1） 電子メールの盗聴対策 電子メールのセキュリティリスクを抑制するには、メールの中に個人を特定できる属性情報を記載しない、どうしても機密情報を記載する必要があるときには、 暗号化し、内容が第三者に漏れないような措置をとる。 現在使用されている電子メールの代表的な暗号化ツールとしては、ハイブリッド方式による暗号化を行うPGPと S/MIMEがある。 （2） 電子メールの改竄対策 中継メールサーバなどで行われる第三者による改竄の脅威に対しては、平文メールのダイジェスト版を作り、これを暗号化して転送する。 受信者のメール改竄を防止するには、ダイジェスト版を送信者の秘密鍵で暗号化するデジタル署名を添付。 平文メールのダイジェスト版作成には、一方向ハッシュ関数による圧縮を行う MD5やSHAを利用し、暗号化については PGPや S/MIMEの利用を考慮すること。 MD5(Message Digest5): RSA暗号を考案したベストによって開発された最も安全性の高いメッセージ圧縮技術である。 SHA(Secure Hash Algorithm): 一方向ハッシュ関数のアルゴリズムで、160ビット(20バイト)のメッセージダイジェストを生成するため、MD5よりもさらに安全性が高い。	マシンレンタルサービスは、貸し出しサーバ上でクライアントが電子メールを利用する場合を想定。

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
							(3) 電子メールのなりすまし対策 電子メールのなりすましの脅威に対処し、そのセキュリティリスクを抑制するには、送信者の正当性を確実に認証できる調停署名も含めた デジタル署名による認証技術を用いる。 PGPには認証局による調停署名(証明書発行や確認)の仕組みがないため、できれば S/MIMEを使用することを考慮すること。 (4) 電子メールの送受信否認防止対策 電子メールの送信否認や受信否認のセキュリティリスクを抑制するためには、調停署名を含めたデジタル署名の仕組みと送信証明書や 受信証明書を発行する認証局のサービスを考慮すること。	
				2) 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること	8.7.4.2	○	1)の項の(1)～(3)の対策の必要性を考慮すること。	監視サービスについては、障害発生等の連絡を対象となる担当者へ連絡する際に電子メールを使用することを想定
				3) 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること	8.7.4.2	×		
				4) 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の	8.7.4.2	×		
				5) 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること	8.7.4.2	○		
				6) 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること	8.7.4.2	○	電子メールの改竄対策を考慮すること。 中継メールサーバなどで行われる再三者による改竄の脅威に対しては、平文メールのダイジェスト版を作り、これを暗号化して転送する。 受信者のメール改竄を防止するには、ダイジェスト版を送信者の秘密鍵で暗号化するデジタル署名を添付すればよい。 平文メールのダイジェスト版作成には、一方向ハッシュ関数による圧縮を行う MD5やSHAを利用し、暗号化については PGPや S/MIMEを利用する。 MD5(Message Digest5): RSA暗号を考案したベストによって開発された最も安全性の高いメッセージ圧縮技術である。	
				7) 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること	8.7.4.2	○	マシンレンタル用サーバでSMTPサービスを利用する場合、送信内容を記録保持するProxyサーバを設置すること。 この場合、プライバシーに配慮し告知などを行うこと。	
			5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入すること	1) 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける情報のぜい(脆)弱性を考慮すること	8.7.5	×		電子オフィスシステムは、監視サービスにおける定期レポート作成の際に使用することを想定。
				2) 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること	8.7.5	×		
				3) 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること	8.7.5	×		
				4) 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること	8.7.5	×		
				5) 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについて	8.7.5	×		
				6) 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮す	8.7.5	×		
				7) 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること	8.7.5	×		
				8) 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること	8.7.5	×		
				9) 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること	8.7.5	×		
				10) 電子オフィスシステムのセキュリティにおいては、緊急時に用いる代替手段についての要求事項及び取決めについて考慮すること	8.7.5	×		
			6) 電子的に公開した情報の完全性を保護するように注意すること	1) 公開されたシステム（例えば、インターネット経由でアクセスできるウェブサーバ）に掲載している情報は、システムが設置された地域又は取引が行われている地域に適用される、法律、規則及び規制に適合する	8.7.5	×		
				2) 情報を公開する前に、正式な認可の手続がとられること	8.7.6	×		
				3) 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって	8.7.6	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				4) 公開している電子システムは、それが情報のフィードバック及び直接入力を許すものである場合には、情報は、あらゆるデータ保護に関連して制定された法律に従って収集するこ	8.7.6	×		
				5) 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること	8.7.6	×		
				6) 取扱いに慎重を要する情報は、収集の過程及び保管時に保護するこ	8.7.6	×		
				7) 公開のシステムにアクセスができても、アクセス権限がないと先のネットワークへのアクセスは、許さないこ	8.7.6	×		
			7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な	1) 音声・画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること	8.7.7	×		
				2) 電話を使うときには、適切な注意を払うことの必要を、職員に意識させること	8.7.7	×		
				3) 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせ	8.7.7	×		
				4) 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残	8.7.7	×		
				5) 職員に、ファクシミリを用いる上での問題点を意識させること	8.7.7	×		
7.1	アクセス制御に関する業務上の	情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定	1) 利用者ごと、または利用者からなるグループごとに対するアクセス制御	9.1.1.1	×		
				2) 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること	9.1.1.1	×		
				3) 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること	9.1.1.1	×		
				4) アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること	9.1.1.1	×		
				5) アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること	9.1.1.1	×		
				6) アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮する	9.1.1.1	×		
				7) アクセス制御に関する個別方針には、異なるシステム及びネットワークにおける、アクセス制御と情報分類の方針との整合性を考慮すること	9.1.1.1	×		
				8) アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること	9.1.1.1	×		
				9) アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用者のアクセス権限情報を考慮すること	9.1.1.1	×		
				10) アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること	9.1.1.1	×		
				11) アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別す	9.1.1.2	×		
				12) アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定す	9.1.1.2	○	マシンレンタル用のサーバで、コンテンツ更新を行う権限を持つユーザやデータの取り出しを行う運用者、システム設定の管理を行う者など作業権限に応じたユーザを新たに作成し、権限を与えること。	
				13) アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をするこ	9.1.1.2	○	マシンレンタル用のサーバで、標準に与えられる権限などでコンテンツ更新に不要な権限（コンテンツ更新エリア以外の書込み権限など）を変更しておくこと。	
				14) アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス権の変更をすること	9.1.1.2	○	マシンレンタル用のサーバでユーザ作成時に、システムから与えられる標準的な権限のテンプレートを使用しないこと。	
				15) アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をする	9.1.1.2	×		
7.2	利用者のアクセス管理	情報システムへの認可されていないアクセスを防止するため	1) 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること	1) 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること	9.2.1	×		
				2) 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者IDを用いること	9.2.1	○	マシンレンタル用のWebサーバでサーバコンテンツ修正のID発行の際には顧客に1つIDを発行するのではなく、利用者別に発行を行うこと。	
				3) 利用者登録手続において、グループIDの使用は、実施される作業に適切な場合にだけ許可すること	9.2.1	○	マシンレンタル用のWebサーバでコンテンツアクセスなどはユーザ毎の運用ルールに基づき、時間制限、アドレス制限などの設定が可能であること、	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査するこ	9.2.1	×		
				5) 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査するこ	9.2.1	×		
				6) 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査するこ	9.2.1	○	マシンレンタル用のサーバでサーバ権限を細分化し、1つのIDで複数の権限を持たせることができないこととすること。	
				7) 利用者登録手続において、重複する利用者IDが別の利用者に発行されないことを確実にすること	9.2.1	○	マシンレンタル用のサーバでID発行時に、最新のユーザ情報との重複の照合を行い、発行が完了してから通知すること。	
				8) 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めることを考慮す	9.2.1	×		
				9) 利用者登録手続において、アクセス権の宣言書を利用者に発行するこ	9.2.1	×		
				10) 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること	9.2.1	×		
				11) 利用者登録手続において、認可手続が完了するまでサービス提供者が利用者にアクセスさせないように	9.2.1	×		
				12) 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること	9.2.1	×		
				13) 利用者登録手続において、職務を変更した利用者、又は組織から離れた利用者のアクセス権を直ちに取り消すこと	9.2.1	×		
				14) 利用者登録手続において、もはや必要のない利用者ID及びアカウントがないか定期的に検査し、あれば削除すること	9.2.1	×		
			2) 特権の割り当て及び使用は、制限し、管理すること	1) 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割当てを管理すること	9.2.2	×		
				2) 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別	9.2.2	×		
				3) 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること	9.2.2	×		
				4) 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと	9.2.2	○	マシンレンタル用のサーバで特権の割り当て時は、設定作業者とは別に、認可者が権限の割り当てに誤りがないか確認を行い、認可を受けてから通知すること。	
				5) 特権の割り当てにおいて、利用者に対する特権の許可が必要ないように、システムルーチンの開発及び使用を促進すること	9.2.2	×		
				6) 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者IDとは別の利用者IDに、割り当て	9.2.2	○	マシンレンタル用のサーバと管理者権限（root）とコンテンツ管理、運用者のIDは兼用にしないこと。	
			3) パスワードの割当ては、正規の管理手続によって統制すること	1) パスワード管理手続の取組において、個人のパスワードを秘密に保つこと	9.2.3	×		
				2) パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に	9.2.3	×		
				3) パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること	9.2.3	○	マシンレンタル用のサーバの採用時にOS、アプリケーションに仮パスワード発行機能があるものを採用し、設定を行うこと。	
				4) パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること	9.2.3	×		
				5) パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること	9.2.3	×		
				6) パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避け	9.2.3	×		
				7) パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること	9.2.3	×		
				8) パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと	9.2.3	○	マシンレンタル用のサーバ上にパスワード情報を管理する場合には暗号化を行い、アクセスを制限すること。	
				9) パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びICカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮	9.2.3	○	マシンレンタル用のサーバで、ユーザ管理に生体認証、トークンやICカードなどより厳密な本人認証を要求された場合、考慮できるよう準備すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
			4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること	1) 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと	9.2.4	×		
				2) 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと	9.2.4	×		
				3) 利用者アクセス権の見直しにおいて、特権の割当てを定期的に検査して、認可されていない特権が取得されてないことを確実にすること	9.2.4	×		
7.3	利用者の責任	認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	1) すべての利用者に、パスワードを秘密にしておくように助言すること	9.3.1	×		
				2) すべての利用者に、パスワードを紙に記録して保管しないように助言すること	9.3.1	×		
				3) すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合は、パスワードを変更するように助言すること	9.3.1	×		
				4) すべての利用者に、最短6文字の質の良いパスワードを選択すること	9.3.1	×		
				5) すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること	9.3.1	×		
				6) すべての利用者に、特権アカウントのパスワードは、通常のパスワードより頻繁に変更するように助言する	9.3.1	×		
				7) すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること	9.3.1	×		
				8) すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること	9.3.1	×		
				9) すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること	9.3.1	×		
				10) すべての利用者に、個人用のパスワードを共有しないように助言する	9.3.1	×		
				11) すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言	9.3.1	×		
			2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護すること	9.3.2	×		
				2) 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること	9.3.2	×		
				3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言する	9.3.2	×		
				4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	9.3.2	×		
				5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	9.3.2	×		
7.4	ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	9.4.1	×		
				2) ネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること	9.4.1	×	顧客のネットワークとそれ以外のネットワークとを適切に分割して定義し、それぞれに対しアクセス権を明確に定めること	技術検証項目ではない
				3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	9.4.1	×	顧客のネットワークとそれ以外のネットワークとを適切に分割して定義し、それぞれに対しアクセス認可の手順を定めること。特にアクセス認可の手順を定める際には、顧客からの承認が必要かどうかを明確にすること	技術検証項目ではない
				4) ネットワークサービスの使用についての個別方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること	9.4.1	×	→全体的記述のため、読替えしない (以下の7.4.2 - 7.4.8までの項での管理策を示しているため、そちらで読替えを行う)	技術検証項目ではない
				5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	9.4.1	×	顧客のネットワークにおける個別方針は業務上のアクセス制御方針と整合していること	技術検証項目ではない

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止する	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	9.4.2	○	→7.4.2項の全体的記述のため、読替えしない。	
				2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	9.4.2	○	顧客のネットワークと顧客企業との接続では、可能な限り専用線を使用すること	
				3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること	9.4.2	○	顧客のネットワークへの接続経路を指定するため、経路制御装置（F/W、ルータACLなど）をインターネットとの接続点、顧客企業との接続点に配置し、指定された業務システムのみにアクセス可能とすること	
				4) 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること	9.4.2	○	？	
				5) 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること	9.4.2	○	顧客のネットワーク内での経路探索を実行させないために、ICMP通信などをインターネットF/Wで通過禁止とすること	
				6) 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること	9.4.2	○	同7.4.2.3	
				7) 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること	9.4.2	○	同7.4.2.3	
				8) 組織内の利用者グループのために別々の論理領域[例えば、仮想私設網（Virtual Private Network：VPN）]を設定することによって、ネットワークアクセスを制限すること	9.4.2	○	顧客のネットワークと顧客企業との接続では、ルータのVPN機能等により機器認証及び暗号化を実施し、ネットワークアクセスを制限すること	
				9) 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと	9.4.2	×		
			3) 遠隔地からの利用者のアクセスには、認証を行うこと	1) コールバックの手順及び制御を用いるとき、組織は、転送機能をもつネットワークサービスを用いないこと	9.4.3	○	？ダイヤルアップによるリモートアクセスを提供する場合は、コールバック機能を使用すること。	転送機能を持つネットワークサービスとは何を意味するか？
				2) 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること	9.4.3	○	？ダイヤルアップによるリモートアクセスを提供する場合は、コールバック機能を使用すること。	転送機能を持つネットワークサービスとは何を意味するか？
				3) コールバックの手順及び制御を徹底的に試験すること	9.4.3	×		
			4) 遠隔コンピュータシステムへの接続は、認証されること	（なし）	9.4.4	○	？	
			5) 診断ポートへのアクセスは、セキュリティを保つように制御されること	1) 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること	9.4.5	○	・レンタル用サーバ及び通信機器におけるメンテナンス通信（ssh,telnet等）は、送信元IPアドレスによるアクセス制御等により保護すること。 また、機器を施錠可能なラックに収められない場合は、シリアルポートに対する不正なケーブル接続を防ぐ措置を講じること。	
				2) ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にすること	9.4.5	×		
			6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること	1) 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること	9.4.6	○	顧客のネットワークとそれ以外のネットワークとの間にセキュリティゲートウェイを配置し、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること	
				2) ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと	9.4.6	×		
				3) 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮すること	9.4.6	×		
			7) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと	1) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること	9.4.7	×		技術検証項目ではない
				2) 電子メールには制限を適用すること	9.4.7	○	7.4.6.1での通信フィルタにおいては、特に以下のプロトコルについて考慮すること ・電子メール ・一方向のファイル転送(FTP) ・双方向のファイル転送（アップロード可能なFTP?） ・対話型アクセス（telnet,sshなど）	
				3) 一方向のファイル転送には制限を適用すること	9.4.7	○	同7.4.7.2	
				4) 双方向のファイル転送には制限を適用すること	9.4.7	○	同7.4.7.2	
				5) 対話型アクセスには制限を適用すること	9.4.7	○	同7.4.7.2	
				6) 時間帯又は日付に対応したネットワークアクセスには制限を適用すること	9.4.7	○	7.5.6.1での通信フィルタにおいては、時間帯又は日付に対応したネットワークアクセスには制限を適用すること	
			8) 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと	1) 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること	9.4.8	○	7.4.6.1での通信フィルタは、発信元及びあて先のIPアドレスに基づいたルールを記述すること	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				2) ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと	9.4.8	×		
			9) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にする	（なし）	9.4.9	×		
7.5	オペレーティングシステムのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること	（なし）	9.5.1	×		
			2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	1) コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること	9.5.2	○	(7.5.2の全体的記述) ・レンタル用サーバ及び通信機器へのログインにおいては、パスワード等の認証機能を必ず使用する。	マシンレンタルサービスにおいては、レンタル用サーバ及び通信機器の ・OS ・ミドルウェア が対象となる
				2) システムについての情報の開示は最小限にすること	9.5.2	○	・レンタル用サーバ及び通信機器へのログイン画面においては、OSの種類／バージョン、ホスト名等のシステム情報、あるいは業務に関する情報（業務名など）を可能な限り表示しないよう設定すること	
				3) ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しな	9.5.2	○	同7.5.2.2	
				4) ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示するこ	9.5.2	○	？（警告を表示することは次項の7.5.2.5-6に反してしまうのではないか？）	
				5) ログオン手順中に、認可されていない利用者の助けとなる表示をしないこと	9.5.2	○	・レンタル用サーバ及び通信機器へのログイン画面においては、前回入力時のユーザIDを表示しないようにすること。また、ログインに失敗した場合には「ログインに失敗した」という旨のみを示すメッセージを表示することとし、「IDが存在しない」、「パスワードが違う」などは表示しない。	
				6) 誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しないこと	9.5.2	○	・レンタル用サーバ及び通信機器へのログイン画面においては、ログインに失敗した場合には「ログインに失敗した」という旨のみを示すメッセージを表示することとし、「IDが存在しない」、「パスワードが違う」などは表示しないようにすること。	
				7) 許容されるログオンの試みの失敗回数を制限すること	9.5.2	○	・レンタル用サーバ及び通信機器へのログインにおいては、ログオン失敗が原則5回以上の連続した場合はロックアウトされるよう設定すること。	
				8) ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと	9.5.2	○	・7.5.2.7のロックアウト機能は原則60分以上経過しないとロックアウトが解除されないように設定すること	
				9) ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること	9.5.2	○	・システム上の制限等で7.5.2.8が実施できない場合は、運用管理者のみがロックアウトを解除できるよう設定し、ロックアウト解除の申請手続きにおいて、必ず運用管理者への認可をとるように定めること	
				10) ログオンの失敗時には、データリンク接続を切ること	9.5.2	○	・レンタル用サーバ及び通信機器への遠隔ログイン（Telnet等）でログオン失敗が3回以上連続した場合はコネクションごと切断するよう設定すること	
				11) ログオン手順のために許容される最長時間及び最短時間を制限すること	9.5.2	○	・レンタル用サーバ及び通信機器への遠隔ログイン（Telnet等）においては、5分以上入力がない場合はコネクションごと切断するよう設定すること。最短時間の制限は、7.5.2.8の管理策を適用する。	
				12) 許容される最長時間及び最短時間の制限から外れる場合、システムはログオンを終了すること	9.5.2	○	同7.5.2.11	
				13) ログオンの失敗時には、失敗した試みを記録すること	9.5.2	○	・レンタル用サーバ及び通信機器へのログインの記録は全て（成功・失敗）ログに保存されるよう設定すること。	
				14) ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること	9.5.2	○	・レンタル用サーバ及び通信機器へのログインに成功した後には、前回ログオンが無事できた日時及び前回のログイン以降失敗したログオンを表示すること。 システム上の利用により実施できない場合は、ログサーバに保存されたログイン記録を定期的に確認するよう手続きを定めること（←運用の話・・）	
				15) ログオンが無事できた時点で、前回のログオン以降、失敗したログオンの試みがある場合は、その詳細を表示すること	9.5.2	○	同7.5.2.14	
			3) すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ID）を保有	1) 利用者IDには、利用者の特権レベル[例えば、管理者(マネージャ)、監督者(スーパーバイザ)]を表示しないこと	9.5.3	○	・（運用の話）レンタル用サーバ及び通信機器への利用者ID名は、命名規則として利用者の特権レベルが分からないようにすること。 システムでデフォルトで作成されるAdministratorなどのIDは名前を変更すること。	
				2) 明らかに業務上の利点がある例外的状況において、利用者のグループ又は特定の業務に対して、共有利用者IDを用いる場合、管理者の承認を文書で得ること	9.5.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			4) 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	1) パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること	9.5.4	×	・レンタル用サーバ及び通信機器では責任の所在を明確にするために、利用者本人のパスワードを使用させること	技術検証項目ではない
				2) パスワードの管理システムでは、適切ならば、利用者に自分のパスワードの選択及び変更を許可し、入力誤りを考慮した確認手順を組み入れること	9.5.4	○	・レンタル用サーバ及び通信機器での利用者パスワードは、利用者本人がパスワード変更を行えるよう設定すること。また入力誤りを考慮し、パスワードを2回入力され同一であることを確認すること。	
				3) パスワードの管理システムでは、質の良いパスワードを選択させるようにすること	9.5.4	○	・レンタル用サーバ及び通信機器での利用者パスワードにおいては、6文字以上で英数字記号の全てが必ず一文字以上使用されているパスワードでないと登録拒否するように設定すること	
				4) パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること	9.5.4	○	・レンタル用サーバ及び通信機器での利用者パスワードにおいては、6ヶ月以上パスワード変更がない場合は、ログイン時にパスワード変更を強制させるよう設定すること。	
				5) パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること	9.5.4	○	・レンタル用サーバ及び通信機器において仮パスワードを使用する場合、仮パスワードは最初のログイン時にパスワード変更を強制させるよう設定すること	
				6) パスワードの管理システムでは、以前の利用者パスワードの記録を、一定期間、維持し再使用を防止すること	9.5.4	○	・レンタル用サーバ及び通信機器では、以前の利用者パスワードの記録を3世代まで記録し、再使用時には変更を強制すること	
				7) パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにすること	9.5.4	○	・レンタル用サーバ及び通信機器では、利用者パスワードの入力時には、パスワードが画面上に表示されないようにすること	
				8) パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること	9.5.4	○	・レンタル用サーバ及び通信機器では、可能であれば認証サーバ等を別途用意しパスワード情報が業務用システムのデータと別に保存されるようにすること。	
				9) パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存すること	9.5.4	○	・レンタル用サーバ及び通信機器では、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードが保存されることを確認すること。	
				10) パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること	9.5.4	○	・レンタル用サーバ及び通信機器では、初期導入時から設定されているパスワード（システムアカウントなど）をすぐに変更すること	
			5) システムユーティリティのために認証手順を使用すること	1) 業務用ソフトウェアからシステムユーティリティを分離すること	9.5.5	○	・レンタル用サーバ及び通信機器では、システム及び業務用ソフトウェアの制御を無効にすることのできるシステムユーティリティ（例：ディスクごとバックアップするツールやレジストリエディタなど）は初期インストールされているものも含め、インストール及び使用を最小限に限定すること	
				2) システムユーティリティの使用を、可能な限り少人数の信頼できる認可された利用者だけに制限すること	9.5.5	○	同7.4.5.1	
				3) システムユーティリティを臨時に使用する際には認可をすること	9.5.5	○	同7.4.5.1	
				4) システムユーティリティの使用の制限をすること	9.5.5	○	同7.4.5.1	
				5) システムユーティリティのすべての使用を記録すること	9.5.5	○	同7.4.5.1	
				6) システムユーティリティの認可レベルの明確化及び文書化をすること	9.5.5	○	同7.4.5.1	
				7) すべての不要なユーティリティソフトウェア及びシステムソフトウェアの除去をすること	9.5.5	○	同7.4.5.1	
			6) 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮する	1) 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと	9.5.6	×		
				2) 脅迫に対する警報に対応する責任及び手順を明確に定めること	9.5.6	×		
			7) リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末	1) 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること	9.5.7	○	？・レンタル用サーバにおいて特に機密性を必要とする業務用ソフトウェアでは、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること	
				2) 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであ	9.5.7	×		
			8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供	1) 既定の時間枠（例えば、バッチファイル伝送のための時間枠）を使うか、又は短時間の通常の対話型処理（session）を用いること	9.5.8	○	？・レンタル用サーバにおいて特に機密性を必要とする業務用ソフトウェアでは、F/W等でアクセス可能な時間帯を制限すること	
				2) 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること	9.5.8	○	？・レンタル用サーバにおいて特に機密性を必要とする業務用ソフトウェアでは、F/W等でアクセス可能な時間帯を就業時間帯に制限すること	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
7.6	業務用ソフトウェアのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	1) 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること	9.6.1	○	OSまたは、各アプリケーションなどのソフトウェアへのアクセスについては、認証などの仕組みによって必ずユーザの正当性が確保されていること。 認証などのプロセスを経由しないアクセスは許可しないこと。 また、認証・認可のポリシーにおいては、組織のアクセス方針に整合していること。	
				2) 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮すること	9.6.1	○	業務用システムでの画面などの表示において、許可されていない機能・メニューなどは表示されないようにすること。 また、現在ログインしているユーザ名（ロール）などが表示されていること。	
				3) 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮	9.6.1	×		
				4) 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること	9.6.1	○	OSまたは、各アプリケーションなどのソフトウェアにおいては、認可などの仕組みを以って、ユーザ毎の読み出し、書き込み、削除、実行などのアクセス権を制限・制御すること。	
				5) 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にすること	9.6.1	○	取り扱いに慎重を要する情報を処理するソフトウェアにおいては、そのソフトウェアからの印刷、メディア出力、画面出力（リモートデスクトップを含む）などの出力を許可された宛先のみに制限すること。 また、それらの出力は、認証などのプロセスを経由したものであること。	
				6) 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること	9.6.1	×		業務・運用
			2) 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること	1) 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること	9.6.2	×		
				2) 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること	9.6.2	×		
7.7	システムアクセス及びシステム使用状況の監視	認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及	1) 監査記録には、利用者IDを含めること	9.7.1	○	監査記録には、利用者IDを確実に含めること。 またそれらの利用者IDは、必ず特定の個人にたどり着けるものであること。	
				2) 監査記録には、ログオン及びログオフの日時を含めること	9.7.1	○	←	
				3) 監査記録には、可能ならば、端末のID又は所在地を含めること	9.7.1	○	監査記録には、端末を確実に識別できるようなID（例：MACアドレスなど）を含めること。	
				4) 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○	監査記録には、システム・データ、他の資源などのへのアクセスについては、成功、失敗にかかわらず、その記録を含めること。	
				5) 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	×		7.7.1.4と重複
			2) 情報処理設備の使用状況を監視する手順を確立すること	1) 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること	9.7.2.1	○	電算室への入退室の監視、またはシステムなどログオン状況の監視について、実行の有無、監視ログの保存期間などは、リスクアセスメントによって決定されること。	
				2) 監視項目には、認可されているアクセスについて、利用者IDを含むこと	9.7.2.1	○	監視項目には、利用者IDを確実に含めること。 また利用者IDは、必ず特定の個人にたどり着けるものであること。	
				3) 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと	9.7.2.1	○	監視項目には、事象がおこった日時を確実に含めること。	
				4) 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと	9.7.2.1	○	監視項目には、行われたオペレーションの種類を確実に含めること。	
				5) 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと	9.7.2.1	○	監視項目には、アクセスされた情報の種類・名称（フォルダ・ファイル名）などを確実に含めること。	
				6) 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと	9.7.2.1	○	監視項目には、使用されたプログラム・ユーティリティ名などを確実に含めること。	
				7) 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること	9.7.2.1	○	監視項目には、特権アカウントで行われた動作については、システムの起動・停止や、入出力装置の取り付け・取り外しを含めて、そのすべてを含めること。	
				8) 監視項目には、すべての特権操作について、システムの起動及び停	9.7.2.1	×		7.7.2.7と重複
				9) 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること	9.7.2.1	×		7.7.2.7と重複
				10) 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること	9.7.2.1	○	監視項目には、認可されていない失敗したアクセスの試みについても、認可されたアクセスと同様の項目を確実に含めること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				11) 監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること	9.7.2.1	○	監視項目には、ネットワークゲートウェイ（ファイウォールを含む）などのアクセス方針違反を確実に含めること。	
				12) 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること	9.7.2.1	×		
				13) 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること	9.7.2.1	○	監視項目には、画面メッセージの発生・その内容などを、システム警告、故障として確実に含めること。	
				14) 監視項目には、システム警告又は故障について、システム記録例外事項を含めること	9.7.2.1	○	監視項目には、例外事項の発生を、システム警告、故障として確実に含めること。	
				15) 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること	9.7.2.1	○	監視項目には、ネットワーク管理警報を、システム警告、故障として確実に含めること。	
			3) 監視の結果は、定期的に見直すこと	1) 監視結果の見直しの頻度は、関係するリスクによって決めること	9.7.2.2	×		
				2) 考慮すべきリスク要因には、業務手続に与える重要性の度合を含める	9.7.2.2	×		
				3) 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること	9.7.2.2	×		
				4) 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること	9.7.2.2	×		
				5) 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること	9.7.2.2	×		
			4) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること	1) セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製するこ	9.7.2.3	○	ログなどについて、重要または緊急とされたものを、選別して閲覧できるような機能を有すること。（例：SIMなどの導入を行う。）	
				2) ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮す	9.7.2.3	×		業務・運用
				3) 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮	9.7.2.3	×		
				4) 記録機能のセキュリティに対して注意すること	9.7.2.3	×	他のコントロールなどを参考にして、syslogサーバなどの運用に留意すること。	他のサブコントロールに網羅されている。
				5) 管理策は、認可されていない変更及び運用上の問題から保護するこ	9.7.2.3	×		業務・運用
			5) コンピュータの時計は正しく設定すること	1) コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時[例えば、万国標準時に（UCT）又は現地の標準時]に合わせること	9.7.3	○	データセンタ内において、標準時（GMT、もしくはローカル）と確実に同期されているNTPサーバを確立すること。また、各サーバは、そのNTPサーバと時刻同期を一定時間ごとに行うこと。	
				2) コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること	9.7.3	○	各サーバ上では、NTPサーバと一定時間ごとに同期処理を行うこと。	
7.8	移動型計算処理及び遠隔作業	移動型計算処理及び遠隔作業の設備を用いるときの情報セキュリティを確実にするため	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特	1) 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること	9.8.1	×		
				2) 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること	9.8.1	×		
				3) 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること	9.8.1	×		
				4) 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと	9.8.1	×		
				5) 悪意のあるソフトウェアに対抗する手順を整えること	9.8.1	×		
				6) 悪意のあるソフトウェアに対抗する手順は最新のものであること	9.8.1	×		
				7) 移動型計算処理を用いる要員に対する訓練を計画すること	9.8.1	×		
				8) 情報を素早く、容易にバックアップできる装置が利用可能となっていること	9.8.1	×		
				9) これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること	9.8.1	×		
				10) 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと	9.8.1	×		
				11) ネットワークに接続された移動型設備の使用に対して適切な保護がなされること	9.8.1	×		
				12) 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されるこ	9.8.1	×		
				13) 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること	9.8.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				14) 大切な、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないこと（可能ならば、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いること）	9.8.1	×		
			2) 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手	1) 遠隔作業の場所に適切な保護が整っていること	9.8.2	×		
				2) 遠隔作業は、経営陣によって認可され、管理されること	9.8.2	×		
				3) 遠隔作業は、この作業形態のため適切に手配されていること	9.8.2	×		
				4) 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること	9.8.2	×		
				5) 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可	9.8.2	×		
				6) 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮	9.8.2	×		
				7) 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮するこ	9.8.2	×		
				8) 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること	9.8.2	×		
				9) 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること	9.8.2	×		
				10) 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報の取扱いに慎重を要する度合を考慮	9.8.2	×		
				11) 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮	9.8.2	×		
				12) 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの情報又は資源への認可されていないアクセスの脅威を考慮する	9.8.2	×		
				13) 遠隔作業活動のための適切な装置を準備すること	9.8.2	×		
				14) 遠隔作業活動のための適切な保管棚・庫の準備をすること	9.8.2	×		
				15) 遠隔作業活動のための許可される作業を明確にすること	9.8.2	×		
				16) 遠隔作業活動のための作業時間を明確にすること	9.8.2	×		
				17) 遠隔作業活動のための保持してもよい情報の分類を明確にすること	9.8.2	×		
				18) 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること	9.8.2	×		
				19) 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること	9.8.2	×		
				20) 遠隔作業を行う場所の物理的なセキュリティを確保すること	9.8.2	×		
				21) 家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引を明確にすること	9.8.2	×		
				22) ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること	9.8.2	×		
				23) バックアップ及び事業継続のための手順を明確にすること	9.8.2	×		
				24) 監査及びセキュリティの監視を行う	9.8.2	×		
				25) 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること	9.8.2	×		
8.1	システムのセキュリティ要求事項	情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には，管理策についての要求事項を明確にするこ	1) セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること	10.1.1	×		
				2) セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				3) 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考	10.1.1	×		
				4) 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				5) 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること	10.1.1	×		
				6) セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること	10.1.1	×		
				7) セキュリティが確保できなかった場合又はセキュリティが確保されていない場合に起こると思われる業務上の損害の可能性もセキュリティ要求事項及び管理策に反映されるこ	10.1.1	×		
8.2	業務用システムのセキュリティ	業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること	1) 業務取引処理(transaction)、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること	10.2.1	×		
				2) 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
			業務システムのセキュリティに関しては「監視サービス」は保留とする	3) データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				4) 入力漏れデータ又は不完全なデータを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				5) データ量の上限及び下限からの超過を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				6) 認可されていない又は一貫しない制御データを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				7) 入力データの妥当性及び完全性を確認するために重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること	10.2.1	×		
				8) 入力データに認可されていない変更があるかどうかについての紙に印刷した入力文書の点検を考慮す	10.2.1	×		
				9) 妥当性確認の誤りに対応する手順について考慮すること	10.2.1	×		
				10) 入力データのもっともらしさを試験する手順について考慮すること	10.2.1	×		
				11) データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること	10.2.1	×		
			2) 処理したデータの改変を検出するために，システムに妥当性の検査を組み込むこと	1) 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること	10.2.2.1	×		
				2) データ変更を行う追加・削除の機能を持つプログラムの使用及びその位置について考慮すること	10.2.2.1	×		
				3) プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること	10.2.2.1	×		
				4) データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮	10.2.2.1	×		
				5) 取引処理の更新後のデータファイルのバランスをとるための処理又はバッチの制御を考慮すること	10.2.2.1	×		
				6) 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること	10.2.2.1	×		
				7) システム生成データの妥当性確認を考慮すること	10.2.2.1	×		
				8) 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること	10.2.2.1	×		
				9) レコード及びファイルの全体のハッシュ合計の検査を考慮すること	10.2.2.1	×		
				10) 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること	10.2.2.1	×		
				11) プログラムが正しい順序で実行されることの検査を考慮すること	10.2.2.1	×		
				12) プログラムが正しい順序で実行されない場合は終了され、問題が解決するまでは処理が停止することを確実に実施しているかの検査を考慮	10.2.2.1	×		
			3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮す	1) メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと	10.2.3	×		
			4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をするこ	1) 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと	10.2.4	×		
				2) 出力データの妥当性確認には、すべてのデータの処理を確実にするための調整制御の回数を含むこと	10.2.4	×		
				3) 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、読取り装置又はその後の処理システムにとっての十分な情報の供給を含むこと	10.2.4	×		
				4) 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと	10.2.4	×		
				5) 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと	10.2.4	×		
8.3	暗号による管理策	情報の機密性、真正性又は完全性を保護するため	1) 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること	1) 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること	10.3.1	×		
				2) 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を	10.3.1	○	運用管理者がシステムにリモートアクセスするような場合には、SSHなどを使用して、通信経路上のデータを暗号化すること。	
			ホスティングに用いるM／Wが暗号化を考慮されている場合△か	3) 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを、	10.3.1	×		運用・業務

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス 対象	マシンレンタルサービス サブコントロール（修正後）	備考（コメント） 想定対象データ等
			接続サービスのVPNが対象となるか？なる場合△	4) 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について、考慮すること	10.3.1	×		運用・業務
				5) 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について、考慮すること	10.3.1	×		運用・業務
				6) 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを、考慮すること	10.3.1	×		運用・業務
				7) 暗号による管理策の使用に関する個別方針を定めるとき、組織全体にわたって効果的に実施するために採用すべき標準類を考慮すること	10.3.1	×		運用・業務
			2) 取扱いに慎重を要する又は重要な情報の機密性を保護するために，暗号化（Encryption）すること	1) リスクアセスメントに基づき、要求される保護レベルを、使用される暗号アルゴリズムの形式及び品質、並びに使用すべき暗号かぎの長さを考慮して明確にすること	10.3.2	×		運用・業務
				2) 組織における暗号利用の個別方針を実施するとき、世界の異なる地域における暗号技術の使用、及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること	10.3.2	×		運用・業務
				3) 暗号技術の輸出入に適用される規制も考慮すること	10.3.2	×		運用・業務
				4) 適切な保護レベルを明らかにするため、及び要求される保護レベルを提供し、かぎ管理機能をもつ安全な製品を選択するために、専門家の助言を求めること	10.3.2	×		運用・業務
				5) 組織が意図した暗号使用に適用される法令及び規制に関して、必要に応じて法律家の助言を求めること	10.3.2	×		運用・業務
			3) 電子文書の真正性及び完全性を保護するために，ディジタル署名を用いること	1) 秘密かぎの機密性を保護するために注意を払うこと	10.3.3	×		
				2) 秘密かぎにアクセスした者は、文書に署名でき、その結果かぎの所有者の署名を盗用することがあり得るため、このかぎを秘密に保管すること	10.3.3	×		
				3) 公開かぎの完全性を保護すること	10.3.3	×		
				4) ディジタル署名に使用される暗号かぎは、暗号化に使用されるものとは異なること	10.3.3	×		
			電子文書の定義 ・業務文書 ・ログを含む監査証跡等 として△とした。	5) ディジタル署名を用いるときは、ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること	10.3.3	×		
				6) 電子商取引の場合、ディジタル署名の法的位置付けを知ること	10.3.3	×		
				7) 法的枠組みが不十分である場合、ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること	10.3.3	×		
				8) 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては、法律家による助言を求めること	10.3.3	×		
			4) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には，否認防止サービスを用いること	（なし）	10.3.4	×		
			5) 一連の合意された標準類，手順及び方法に基づくかぎ管理システムを，暗号技術の利用を支援するために用いること	1) 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること	10.3.5.1	○	←	
				2) すべてのかぎは、変更及び破壊から保護し、共通かぎ及び秘密かぎは、認可されていない露呈から保護すること	10.3.5.1	○	すべてのかぎは、ファイルシステムでのアクセス権などによって、そのセキュリティが保持されていること。	
				3) かぎを生成し、保存し、記録保管するために用いられる装置を保護するためには、物理的保護策を用いること	10.3.5.1	○	かぎ生成、保管を行うサーバなどについては、物理入退室の管理された設備や、施錠されたラックに設置するなど、保護されていること。	
				4) かぎ管理システムでは、種々の暗号システム及び種々の業務用ソフトウェアのためのかぎを生成する方法を定めること	10.3.5.1	×		業務・運用
			鍵の必要な暗号 ・データ保存 ・通信暗号（共通鍵） ・ログ保存 とした	5) かぎ管理システムでは、公開かぎ証明書を生成し入手する方法を定めること	10.3.5.1	×		業務・運用
				6) かぎ管理システムでは、予定している利用者にかぎを配付する方法を定めること	10.3.5.2	×		業務・運用
				7) かぎ管理システムでは、かぎを保存する方法を定めること	10.3.5.2	○	かぎは、電子ファイルとしては、ファイルシステムのアクセス権などによって、また媒体などにおいては、耐タンパ性の高いものなどに保存することによって、確実に保護され	
				8) かぎ管理システムでは、かぎを変更又は更新する方法を定めること	10.3.5.2	×		業務・運用
				9) かぎ管理システムでは、セキュリティが損なわれたかぎを処理する方法について定めること	10.3.5.2	○	かぎについて、電子ファイルであれば確実な削除、媒体であれば、粉砕などによって、確実に処理を行うこと。	
				10) かぎ管理システムでは、かぎを無効にする方法について定めること	10.3.5.2	○	PKIでは、失効リストなどを確実に運用すること。	
				11) かぎ管理システムでは、事業継続管理の一部として、例えば、暗号化された情報の回復のために、消失したかぎ又は損傷したかぎを回復する方法を定めること	10.3.5.2	○	←	？？

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				12) かぎ管理システムでは、かぎを、例えば、記録保管された情報又はバックアップされた情報などのために、記録保管する方法について定める	10.3.5.2	×	かぎ管理システムでは、データバックアップなどを確実に行うこと。	マシンレンタルでは対象外
				13) かぎ管理システムでは、かぎを破壊する方法を定めること	10.3.5.2	○	かぎについて、電子ファイルであれば確実な削除、媒体であれば、粉砕などによって、確実に処理を行うこと。	
				14) かぎ管理システムでは、かぎ管理に関連する活動を記録し監査する方法を定めること	10.3.5.2	○	かぎの生成・廃棄などについては、そのことをログに残すこと。	
				15) かぎ管理システムでは、セキュリティが損なわれる可能性を軽減するために、かぎは一定期間だけ用いることができるように、かぎの活性化及び非活性化の期日を定めるこ	10.3.5.2	×		業務・運用
				16) かぎの活性化及び非活性化の期間は、暗号による管理策が使用される環境及び認識されているリスクに	10.3.5.2	×		業務・運用
				17) 安全に管理された共通かぎ及び秘密かぎの問題に加え、公開かぎの保護についても考慮すること	10.3.5.2	×	LDAPサーバなどで公開かぎを公開している場合には、そのセキュリティに留意すること。	マシンレンタルでは対象外
				18) 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に	10.3.5.2	×		業務・運用
8.4	システムファイルのセキュリティ	ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため	1) 運用システムでのソフトウェアの実行を管理すること	1) 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること	10.4.1	○	SNMPエージェントソフトの更新（設定変更およびPTFの適用等）は、適切な管理者の承認を受けた、サーバ管理者により実施されること。	
				2) 運用システムは、実行可能なコードだけを保持すること	10.4.1	○	SNMPエージェントソフトは、実行可能なオブジェクトのみマシンレンタル用サーバ内に保持し、ソースコードは保持しないこと。	⇒通常のパッケージソフトのソースは保持すること事態が困難であるが敢えて記載した
				3) 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れの確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しな	10.4.1	○	SNMPエージェントソフトに対する設定変更、PTFの適用は、管理者の承認を受け、作業指示が出されるまで実行しないこと。	
				4) 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること	10.4.1	○	SNMPエージェントソフトの更新（設定変更およびPTFの適用等）については、操作記録取得ソフトで、証跡を残し管理すること。	
				5) 古い版のソフトウェアは、事故対策用として保持すること	10.4.1	○	SNMPエージェントソフトの更新（設定変更およびPTFの適用等）を行う際は、旧バージョンおよび更新前の設定内容のバックアップを取得すること。	
				6) 運用システムに使用されるベンダー供給ソフトウェアは、供給者によって支援されるレベルで、維持管理されること	10.4.1	○	SNMPエージェントソフトは、ベンダーが提供するバージョンを使用し、独自に変更および改良を加えないこと。	
				7) 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数	10.4.1	○	OSおよびSNMPエージェントソフトのバージョンアップの際には、業務要件のみならず、セキュリティ機能の適用可否についても考慮すること。	
				8) セキュリティ上の欠陥を除去するか又は軽減するのに役立つ場合には、ソフトウェアパッチを適用すること	10.4.1	○	OSのセキュリティパッチの適用可否を判断し、必要であればパッチの適用を実施すること。	
				9) 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること	10.4.1	○	マシンレンタル用サーバに対して、供給者が作業をする場合は、S社のサーバ管理者が立会い、管理者IDでログイン後の状態で提供すること。（原則として供給者には、管理者IDおよびパスワードを提供しないこと）	
				10) 供給者の活動は監視されることが望ましい	10.4.1	○	供給者がサーバルームへ立ち入る場合は、S社の担当者が帯同するか、監視カメラ等で作業状況を監視すること。	
			2) 試験データを保護し，管理すること	1) システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと	10.4.2	×		試験データおよび本番データは、委託元の資産であるため、S社の管理下にはな
				2) 個人情報が入っている運用データベースは、使用しないようにすること	10.4.2	×		同上
				3) 個人情報が入っている情報を使用する場合は，使用する前に，個人的要素を消去すること	10.4.2	×		同上
				4) 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用	10.4.2	×		同上
				5) 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けるこ	10.4.2	×		同上
				6) 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること	10.4.2	×		同上
				7) 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること	10.4.2	×		同上
			3) プログラムソースライブラリへのアクセスに対しては，厳しい管理を維持す	1) 可能な限り、プログラムソースライブラリは、運用システムに含めないこと	10.4.3	×		
				2) 各アプリケーションごとに、プログラムライブラリ管理責任者を任命する	10.4.3	×		
				3) IT支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと	10.4.3	×		
				4) 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと	10.4.3	×		
				5) その業務用ソフトウェアのためのIT支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プログラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること	10.4.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) プログラムリストは、セキュリティの保たれた環境に保持されること	10.4.3	×		
				7) プログラムソースライブラリへのすべてのアクセスについて、監査記録を維持管理すること	10.4.3	×		
				8) ソースプログラムの旧版は、記録保管しておくこと	10.4.3	×		
				9) 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと	10.4.3	×		
				10) プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従うこと	10.4.3	×		
8.5	開発及び支援過程におけるセキュリティ	業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理すること	1) 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないこと	10.5.1	○	OS、SNMPエージェントソフトの変更、更新は、事前に定められた手順に沿って実施すること。	
				2) 支援プログラマによるシステムへのアクセスはその作業に必要な部分に限定されること	10.5.1	×		マシンレンタルサービスは個別開発のアプリケーションを対象としないため、プロ
				3) 変更に対する正式な合意及び承認が得られていることを確実にするこ	10.5.1	×		技術ではないので、×とする
				4) 業務用ソフトウェア及び運用の変更管理手順は統合されること	10.5.1	×		マシンレンタルサービスでは、業務用ソフトウェアは対象としないので、×とする。SNMPエージェントソフトは、別項のパッケージソフトの
				5) 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること	10.5.1	×		同上
				6) 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確	10.5.1	×		同上
				7) 業務用ソフトウェア及び運用の変更過程では、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするためにこの手順をレビューすること	10.5.1	×		同上
				8) 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識	10.5.1	×		同上
				9) 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を	10.5.1	×		同上
				10) 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること	10.5.1	×		同上
				11) 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること	10.5.1	×		同上
				12) 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新さ	10.5.1	×		同上
				13) 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実に	10.5.1	×		同上
				14) 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェアの更新について版数の管理を行うこと	10.5.1	×		同上
				15) 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること	10.5.1	×		同上
				16) 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること	10.5.1	×		同上
				17) 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること	10.5.1	×		同上
			2) オペレーティングシステムを変更した場合は，業務用システムをレビューし，試験すること	1) オペレーティングシステムの変更によって業務用ソフトウェアの管理及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること	10.5.2	○	マシンレンタル用サーバのOSのバージョンアップ、PTFの適用等については、実行手順を責任者のレビューを受けること。	
				2) 年間支援計画及び予算には、オペレーティングシステムの変更の結果として必要となるレビュー及びシステム試験を必ず含めるようにするこ	10.5.2	×		技術ではないので、×とする
				3) 実施前に行う適切なレビューに間に合うように、オペレーティングシステムの変更を通知することを確実にす	10.5.2	×		技術ではないので、×とする
				4) 事業継続計画に対して適切な変更がなされることを確実にすること	10.5.2	○	マシンレンタル用サーバのOSのバージョンアップ、PTFを実行した場合は、バックアップ用のサーバに対しても同様の作業を実施すること。	
			3) パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更を厳しく管理すること	1) ベンダー供給のパッケージソフトウェアは、変更しないで使用すること	10.5.3	○	SNMPエージェントソフトは、パッケージで供給された機能のよる設定を行い、ソースレベルでの変更は行わないこと。	
				2) パッケージソフトウェアの変更が絶対必要であると判断された場合は、組み込まれている管理策及び完全性の処理が損なわれるリスクを考	10.5.3	○	SNMPエージェントソフトを変更する場合は、ソフトウェアの機能のみならず、監視業務全体の業務プロセスに対する影響度を評価すること。	
				3) パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること	10.5.3	○	SNMPエージェントソフトの変更を行う際、オリジナルプログラムへの改良が契約上可能であるか確認し、必要であればベンダーに同意を得ること。	
				4) パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる	10.5.3	○	SNMPエージェントソフトの変更を行う際、ベンダーが提供する修正用プログラムの有無および適用可否を検討すること。	
				5) パッケージソフトウェアの変更が絶対必要であると判断された場合は、変更の結果として、将来のソフトウェア保守に対して組織が責任を負うようになるかどうかの影響を考慮すること	10.5.3	○	SNMPエージェントソフトの変更を行った際、変更後の状態で、将来的にソフトウェア自体のバージョンアップが発生した場合に対応できるよう、個別変更内容の詳細を記録して、組織として継続的に管理すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				6) 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと	10.5.3	○	SNMPエージェントソフトの変更を行う際は、バックアップを取得し、オリジナルを適切に保管してから複製に対して変更を行うこと。	
				7) 変更はすべて、完全に試験すること	10.5.3	○	SNMPソフトウェアを変更する際は、監視業務で使用する機能すべてをテストすること。	
				8) 変更はすべて、文書化すること	10.5.3	○	SNMPソフトウェアを変更する際は、変更した内容の詳細を適切に記録しう文書化すること。	
				9) 将来更新されたソフトウェアに再び適用できるようにすること	10.5.3	○	SNMPエージェントソフトの変更を行った際、変更後の状態で、将来的にソフトウェア自体のバージョンアップが発生した場合に対応できるよう、個別変更内容の詳細を記録して、組織として継続的に管理すること。	
			4) 隠れチャネル（Covert channels）及びトロイの木馬（Trojan code）の危険性から保護するために，ソフトウェアの購入，使	1) プログラムは定評のある開発元のものだけを購入すること	10.5.4	○	SNMPエージェントソフトを購入する際は、正規の販売されているソフトを購入し、フリーソフトウェア等は、使用しないこと。	
				2) コードの確認ができるようにソースコードでプログラムを購入すること	10.5.4	○	プログラムの開発を外部へ委託する場合は、ソースコードの納入を受けること。	通常のパッケージソフトをソースで購入することは現実的に難しいと考える。
				3) 評価された製品を用いること	10.5.4	○	購入するソフトウェアは、第三者の適合評価を受けた製品であること。	
				4) 使用前にすべてのソースコードを検査すること	10.5.4	○	外部委託先が開発したプログラムを受け入れる場合は、不正なコードが含まれていないか検査をすること。	通常のパッケージソフトをソースで購入することは現実的に難しいと考える。
				5) 一旦導入したコードへのアクセス及びそのコードへの変更を管理するこ	10.5.4	○	外部委託先が開発したプログラムを受け入れる場合は、導入後の変更についても管理すること。	通常のパッケージソフトをソースで購入することは現
				6) 重要なシステムでの作業には確実に信頼できる要員を用いること	10.5.4	×		技術ではないので、×とする
			5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために，管理策を用いるこ	1) ソフトウェア開発を外部委託する場合、使用許諾に関する取決め、コードの所有権及び知的所有権について考慮すること	10.5.5	×		
				2) ソフトウェア開発を外部委託する場合、実施される作業の質及び正確さの認証を考慮すること	10.5.5	×		
				3) ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託（escrow）契約に関する取決めについて考慮すること	10.5.5	×		
				4) ソフトウェア開発を外部委託する場合、なされた作業の質及び正確さの監査のためのアクセス権について	10.5.5	×		
				5) ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること	10.5.5	×		
				6) ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること	10.5.5	×		
9.1	事業継続管理の種々の面	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護	1) 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が	1) 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること	11.1.1	×		
				2) 業務手続の中断が事業に及ぼすと思われる影響を理解し（組織の存続性を脅かす可能性のある重大な事件・事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である）、情報処理施設の事	11.1.1	×		
				3) 事業継続の手続の一部をなすこともある適切な保険への加入を考慮	11.1.1	×		
				4) 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること	11.1.1	×		
				5) 合意された戦略に従って事業継続計画を明確にし、文書化すること	11.1.1	×		
				6) 実行されている計画及び手続を定期的に試験し、更新すること	11.1.1	×		
				7) 事業継続管理が組織の手続及び機構に確実に組み込まれるようにする	11.1.1	×		
				8) 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること	11.1.1	×		
			2) 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特	1) それらの障害の影響（損害規模及び回復期間の両面から）を判断するために、リスクアセスメントを行うこ	11.1.2	×		
				2) これら両活動の実施には、事業資源及び手続の管理者が全面的に関	11.1.2	×		
			3) 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てるこ	1) 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること	11.1.2	×		
			4) 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるため	1) 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること	11.1.3	×		
				2) 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施す	11.1.3	×		
				3) 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に	11.1.3	×		
				4) 事業継続計画の作成過程では、合意された手順及び過程を文書化す	11.1.3	×		
				5) 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと	11.1.3	×		
				6) 事業継続計画の作成過程では、計画の試験及び更新を行うこと	11.1.3	×		
				7) 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと	11.1.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				8) これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること	11.1.3	×		
			5) すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組	1) 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること	11.1.4	×		
				2) 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正す	11.1.4	×		
				3) 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件	11.1.4	×		
				4) 事業継続計画作成の枠組みでは、事業運営及び/又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること	11.1.4	×		
				5) 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決	11.1.4	×		
				6) 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の	11.1.4	×		
				7) 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること	11.1.4	×		
				8) 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表につい	11.1.4	×		
				9) 事業継続計画作成の枠組みでは、事業継続手続を理解させ、手続が継続して有効であることを確保するために計画される認識及び教育活動について考慮すること	11.1.4	×		
				10) 事業継続計画作成の枠組みでは、個人の責任について考慮すること	11.1.4	×		
				11) 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するのに誰が責任をもつかを記述すること	11.1.4	×		
				12) 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること	11.1.4	×		
				13) 事業継続計画作成の枠組みでは、各計画には特定の責任者がいるこ	11.1.4	×		
				14) 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること	11.1.4	×		
				15) 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者	11.1.4	×		
			6) 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的	1) 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職員がそれらの計画を確実に認識するものであること	11.1.5.1	×		
				2) 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと	11.1.5.1	×		
				3) 計画の個々の構成要素を、頻繁に試験すること	11.1.5.1	×		
				4) 計画が実際に役立つことを保証するために、様々な手法を使用するこ	11.1.5.1	×		
				5) 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画	11.1.5.1	×		
				6) 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）	11.1.5.1	×		
				7) 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）	11.1.5.1	×		
				8) 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施す	11.1.5.1	×		
				9) 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）	11.1.5.1	×		
				10) 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験す	11.1.5.1	×		
				11) いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反	11.1.5.1	×		
			7) 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって	1) 事業継続上の問題を適切に対処することを確実にするための手順は、組織の変更管理プログラムの中に含まれること	11.1.5.2	×		
				2) 各事業継続計画の定期的見直しに対する責任を割り当てること	11.1.5.2	×		
				3) 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に	11.1.5.2	×		
				4) この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること	11.1.5.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
10.1	法的要求事項への適合	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項に適合する特定の管理策、及び個々の責任も同様に明確	12.1.1	×		
			2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は，法的制限事項に適合するよう	1) ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること	12.1.2.2	×		
				2) ソフトウェア製品の取得手続に関する標準類を発行すること	12.1.2.2	×		
				3) ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること	12.1.2.2	×		
				4) 適切な財産登録簿を維持管理する	12.1.2.2	×		
				5) 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること	12.1.2.2	×		
				6) 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること	12.1.2.2	×		
				7) 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確認すること	12.1.2.2	○	インベントリ管理ツールにより、認可していないソフトウェアが導入されていないことを定期的に確認すること。	
				8) 適切な使用許諾条件を維持管理するための個別方針を定めること	12.1.2.2	○	インベントリ管理ツールにより導入しているソフトウェアのライセンス管理を行うこと。	
				9) ソフトウェアの処分又は他人への譲渡についての個別方針を定めること	12.1.2.2	×		
				10) 適切な監査ツールを用いること	12.1.2.2	×		
				11) 公衆ネットワークから入手するソフトウェア及び情報の使用条件に従うこ	12.1.2.2	×		
			3) 組織の重要な記録は、消失、破壊及び改ざんから保護されること	1) 記録類は、記録の種類（例えば、会計記録、データベース記録、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について保持期間及び記録媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光学媒体）の詳細も定めておく	12.1.3	×		
				2) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること	12.1.3	○	マシンをレンタルしている顧客がオーナーの情報として暗号化された情報がある場合は、顧客側が適切な管理を行うよる依頼し、S社のサーバ管理者は、顧客より指示が無い限りアクセスしないこと。	
				3) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、必要なときに、認可されている者が使用できるようにすること	12.1.3	○	マシンをレンタルしている顧客がオーナーの情報として暗号化された情報がある場合は、顧客側が適切な管理を行うよる依頼し、S社のサーバ管理者は、顧客より指示が無い限りアクセスしないこと。	
				4) 記録の保管に用いられる媒体が劣化する可能性を考慮すること	12.1.3	×		
				5) 保管及び取扱いの手順は、製造業者の推奨に従って実行すること	12.1.3	×		
				6) 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確保する手順を	12.1.3	×		
				7) 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式で取り出すことができるように、データ保管システムを選択すること	12.1.3	×		
				8) 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にす	12.1.3	×		
				9) 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること	12.1.3	×		
				10) 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行す	12.1.3	×		
				11) 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること	12.1.3	×		
				12) 主要な情報の出典一覧を維持管理すること	12.1.3	×		
				13) 重要な記録及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実行すること	12.1.3	○ サーバーシ	サーバーで取得しているログ情報は、適切な保護下にあるログサーバに随時収集され、改ざんから保護すること。	
			4) 関連する法令に従って個人情報を保護するために，管理策を用いること	1) データ保護の担当責任者を任命すること	12.1.4	×		
				2) 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当責任者に報告することは、データ所有者の責任であること	12.1.4	×		
				3) 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任で	12.1.4	×		
			5) 情報処理施設の使用には管理者の認可を要するものとし，そのような施設の誤用を防ぐための	1) 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされ	12.1.5	×		
				2) 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること	12.1.5	×		
				3) 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること	12.1.5	×		
				4) すべての利用者は、その許可されたアクセスの正確な範囲を認識して	12.1.5	×		
				5) 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを	12.1.5	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	マシンレンタルサービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告メッセージをコンピュータの画面上に表	12.1.5	○	マシンレンタルとして、維持管理が必要な、OS、ミドル、監視、バックアップ等の管理系ソフト以外にアクセスしようとした場合は、警告メッセージを表示させること。	
				7) 利用者は、引き続きログオン処理を行うために画面上のメッセージに同意し、それに適切に対応すること	12.1.5	×		
			6) 暗号による管理策の策定においては、国の法律への適合を確実なものにするために、法的な助	1) 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること	12.1.6	×		
			7) 人又は組織に対する措置を支援するには，十分な証拠をもつこと	1) 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること	12.1.7.1	×		
				2) 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとる	12.1.7.1	×		
				3) 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること	12.1.7.3	○	オリジナルの文書には、朱色印を押すとう、複製防止の措置を講じること。	
				4) コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっ	12.1.7.3	×		
				5) コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること	12.1.7.3	×		
				6) コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること	12.1.7.3	×		
				7) 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得る	12.1.7.3	×		
10.2	セキュリティ基本方針及び技術適合のレビュー	組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため	1) 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にす	1) 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること	12.2.1	×		
				2) 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること	12.2.1	×		
			2) 情報システムは，セキュリティ実行標準と適合していることを定期的に検査すること	1) 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行	12.2.2	○	マシンレンタル用サーバのOS、ミドルの設定が、S社の定めるセキュリティスタンダード、プロシージャに適合していることを点検すること。	
				2) 技術適合の検査では、専門家の技術援助を得ること	12.2.2	×		
				3) 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアによって実施されるこ	12.2.2	○	マシンレンタル用サーバのOS、ミドルがS社の定めるセキュリティスタンダード、プロシージャに技術的に適合していることを確認するため、監査用ソフトウェア等を用いて確認する。確認する内容の例としては、セキュリティに関するOS上のパラメタ設置または、パスワードの設定状況等が考えられる。	
				4) 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること	12.2.2	×		
				5) いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施さ	12.2.2	×		
10.3	システム監査の考慮事項	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重	1) 監査要求事項は、担当経営陣の同意を得ること	12.3.1	×		
				2) 検査の範囲は、合意され、管理されること	12.3.1	×		
				3) 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定するこ	12.3.1	×		
				4) 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること	12.3.1	×		
				5) 複製ファイルは、監査が完了した時点で消去すること	12.3.1	×		
				6) 検査を実施するための情報資源は、明確に識別され、利用可能であ	12.3.1	×		
				7) 特別又は追加処理の要求事項は、識別され、合意されること	12.3.1	×		
				8) すべてのアクセスは、照合用の証跡を残すために、監視され、記録さ	12.3.1	×		
				9) すべての手順、要求事項及び責任について、文書化すること	12.3.1	×		
			2) システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護さ	1) システム監査ツールは、開発及び運用システムから分離しておくこと	12.3.2	×		
				2) システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと	12.3.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
5.2	装置のセキュリティ	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	1) 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること	1) 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること	7.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類はラックなどに収納し、施錠を行うこと。	ここでは、各サービスにおける次の装置等を想定する。
				2) 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること	7.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の管理コンソール画面にはフィルタを設置し、視認できる範囲を限定すること。 コンソールはラック内に設置し、作業中も周囲の目からできる限り制限すること。	・マシンレンタルサービス：レンタル用サーバおよび通信機器。
				3) 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること	7.2.1	○	接続サービス用の装置類は、ユーザレンタル用の装置類と分離されて設置されること。	・接続サービス：インターネット接続に必要な、FWサーバおよびルータ等の通信機器。
				4) 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の策定を考慮すること	7.2.1	×		・監視サービス：監視用の端末等
				5) 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること	7.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類を設置するラックには温湿度監視装置を設置し、最も環境条件の弱い機器に対応した管理を実施すること。温湿度はデータセンターの機器管理室で常時監視し異常時はアラームが上がる仕組みを持たせること。	・ファシリティ：入退館管理装置、監視カメラ等
				6) 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること	7.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のメンテナンス作業にはその都度接続するメンテナンスコンソールを用い、常時キーボード等の周辺機器は接続しておかないこと。どうしても接続したままにする場合は、キーボード、電源スイッチ、モード切替のボタン等には、誤って、不用意な操作が行わないようカバー等で保護すること。	
				7) 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること	7.2.1	×		
			2) 装置は、停電、その他の電源異常から保護すること	1) 装置は、装置製造者の仕様に適合した適切な電力の供給を確保すること	7.2.2	×		
				2) 電源の多重化をすること	7.2.2	×		
				3) 無停電電源装置（UPS）を設置する	7.2.2	×		
				4) 非常用発電機の設置をすること	7.2.2	×		
				5) 障害対策計画では、UPSが故障した場合に取るべき措置についても計画しておくこと	7.2.2	×		
				6) UPSは、容量が十分であることを定期的に確認すること	7.2.2	×		
				7) UPSは、製造者の推奨に従って点検すること	7.2.2	×		
				8) 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること	7.2.2	×		
				9) 発電機を使用する場合、製造者の推奨に従って定期的に点検すること	7.2.2	×		
				10) 発電機を長時間運転できるように、燃料の十分な供給を確保すること	7.2.2	×		
				11) 電源の緊急スイッチは、機械室の非常口近くに設置すること	7.2.2	×		
				12) 主電源の停電時用として非常用照明を備えること	7.2.2	×		
				13) 落雷防護はすべての建物に備えること	7.2.2	×		
				14) すべての外部通信回線に落雷防護フィルタを付けること	7.2.2	×		
			3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護すること	1) 情報処理設備に接続する電源ケーブル及び通信回線は、可能ならば地下に埋設するか、又はそれに代わる十分な保護手段を施すこと	7.2.3	×		
				2) ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること	7.2.3	○	ユーザレンタルエリア外にネットワークケーブルを設置し、さらに管路内に設置することで、容易に触れないように保護すると共に、漏洩電波(メタル線の場合)などが漏れないように処置すること。	ネットワークケーブルに関する管理は、各サービスに付随するハードウェアの一部として、各サービス毎に振り下げる
				3) 干渉を防止するために、電源ケーブルは通信ケーブルから隔離すること	7.2.3	○	電源と通信ケーブルは管路を分離するか、シールドなどの保護を行うこと。	
				4) 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること	7.2.3	○	ユーザレンタルエリアとは区別した上で、重要機能を有する機器は他の機器のケーブルとは別に外装電線管などを用いて損傷などから保護すること。	
				5) 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること	7.2.3	○	ユーザレンタルエリアとは区別した上で、通信ケーブルの接続部分などは修正が行われないようカバーなどを付けて施錠、封印を行うこと。	
				6) 取扱いに慎重を要するシステム又は重要なシステムに対しては、代替経路又は伝送媒体を使用すること	7.2.3	○	接続サービスに用いるF/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類は常用待機、負荷分散などの冗長構成を採ること。	
				7) 取扱に慎重を要するシステム又は重要なシステムに対しては、光ファイバケーブルを使用すること	7.2.3	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の接続には極力光ファイバーケーブルを用い、メタル線を利用する場合はシールド処理を行うこと。	
				8) 認可されていない装置がケーブルに取り付けられているかどうかについての調査すること	7.2.3	○	検疫ネットワークシステムを導入し、認可されていない装置が接続されるのを防ぐこと。検疫ネットワークが導入できない場合は、スイッチなどの接続ポートで使用していないものは無効設定とするか、封印を行い使用されていないか定期的に確認すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
			4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること	1) 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること	7.2.4	○	通信システムのエラーチェック等を定期的に実施するよう保守スケジュールを管理するシステム、あるいはCronなどを利用して実施時期の自動通知機能を設定すること。	技術的検証項目にあらず
				2) 認可された保守担当者だけが装置の修理及び手入れを実施すること	7.2.4	○	保守担当者と担当する作業内容について事前の申請を行い、ネットワーク機器管理者の認可を受けること。 作業時には、サーバ管理者、サーバ管理者に権限を委譲された者が監督を行うこと。	技術的検証項目にあらず
				3) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること	7.2.4	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の保守作業中の内容についてコマンドなどの記録を行い、作業終了後、実施作業の検証を行うこと。	技術的検証項目にあらず
				4) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること	7.2.4	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のシステムログに障害に関する情報が記録されていること。 障害時の保守記録について対応記録をネットワーク機器設置場所とは別に保管されていること。	技術的検証項目にあらず
				5) 装置を保守するために搬出する場合、適切な管理策を施すこと	7.2.4	○	搬出時にはデータのバックアップを実施後、消去を実施、確認されていること。	技術的検証項目にあらず
				6) 保険約款によって定められたすべての要求事項に従うこと	7.2.4	×		
			5) 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可すること	1) 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること	7.2.5	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等のメンテナンス作業のために接続する場合、情報の盗聴等を防止する為にVPN等で通信の暗号化を図ること。さらに、万が一の事態に備え、サービスをバックアップルートに切り替えるか、サービスを停止させた上で実施すること。	接続サービス、監視サービスにおいて、専門家が自宅よりリモート接続して操作することを想定している。
				2) 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと	7.2.5	○	保守用端末を持ち出して作業する場合は、持ち出しの規定に則った運用を行うこと。	技術的検証項目にあらず
				3) ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること	7.2.5	○	ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること。	技術的検証項目にあらず
				4) 装置の保護に関しては、製造者の指示に常に従うこと	7.2.5	○	保守用端末を持ち出して作業する場合は、持ち出しの規定に則った運用を行うこと。	技術的検証項目にあらず
				5) 在宅作業についての管理策は、リスクアセスメントによって決定すること	7.2.5	○	保守用端末を持ち出して作業する場合は、持ち出しの規定に則った運用を行うこと。	技術的検証項目にあらず
				6) 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること	7.2.5	○	在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること	技術的検証項目にあらず
				7) 事業所外の装置を保護するために、十分な保険が付保されていること	7.2.5	○	持ち出し機器については、盗難保険などに加入すること。	技術的検証項目にあらず
				8) セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること	7.2.5	○	遠隔保守作業は決められた場所以外では実施しないこと。	技術的検証項目にあらず
			6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること	1) 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること	7.2.6	○	ディスク廃棄やサーバ障害などのディスク交換時にデータの残留検査を実施すること	ファシリティでは、生態認証の情報等を想定している。
				2) 取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアが、消去又は上書きされているか確認すること	7.2.6	○	公開コンテンツの情報以外のサーバの設定情報やアカウントの情報など、機密性を重要とされるデータは消去、上書きを実施していること。	
5.3	その他の管理策	情報及び情報処理設備の損傷又は盗難を防止するため	1) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮すること	1) クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること	7.3.1	×		
				2) クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること	7.3.1	×		
				3) 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管すること	7.3.1	×		
				4) 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと	7.3.1	×		
				5) パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと	7.3.1	×		
				6) パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること	7.3.1	×		
				7) 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること	7.3.1	×		
				8) 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと	7.3.1	×		
				9) 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと	7.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			2) 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできな	1) 持出し時及び返却時に記録を残すこと	7.3.2	×		
				2) 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること	7.3.2	×		
				3) 現場検査があることを各人が認識していること	7.3.2	×		
6.1	運用手順及び責任	情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと	1) 操作手順は、正式な文書として取り扱うこと	8.1.1	×		ファシリティでは、入退室管理、各種制御系システムを想定。
				2) 操作手順が変更の場合は管理者によって認可されること	8.1.1	×		
				3) 操作手順には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				4) 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記	8.1.1	×		
				5) 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記	8.1.1	×		
				6) 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				7) 操作手順には、特別な出力の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記す	8.1.1	×		
				8) 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				9) 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること	8.1.1	×		
			2) 情報処理設備及びシステムの変更について管理すること	1) 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること	8.1.2	×		
				2) 運用プログラムは、厳重な変更管理の下に置くこと	8.1.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定等の変更に関しては、ユーザ認証による変更管理権限を持たせて制限すること。	
				3) プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること	8.1.2	○	監査記録は改ざんなどを行われないようにするため別のサーバへの転送、ハッシュをとるなどの処理を行うこと。	技術検証項目にあらず
				4) 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合するこ	8.1.2	×		
				5) 重要な変更を識別及び記録すること	8.1.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更は、ファイルアクセス履歴として収集し、別途設置するログ管理サーバに署名つきログとして保管、管理すること。ログは定期的なバックアップが取られること。	
				6) 重要な変更の潜在的な影響の評価をすること	8.1.2	×		
				7) 変更の申出を正式に承認する手順を確立すること	8.1.2	×		
				8) 変更の詳細の、全関係者への通知をすること	8.1.2	×		
				9) うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること	8.1.2	×		
			3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立すること	1) 情報システムの故障及びサービスの停止に対処できるように、手順を定めること	8.1.3	×		
				2) サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること	8.1.3	×		
				3) 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること	8.1.3	×		
				4) 機密性に対する違反に対処できるように、手順を定めること	8.1.3	×		
				5) 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を	8.1.3	×		
				6) 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること	8.1.3	×		
				7) 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること	8.1.3	×		
				8) 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること	8.1.3	×		
				9) 通常の障害対策計画手順には、監督機関に対する措置の報告を含め	8.1.3	×		
				10) 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のアクセスログ、通信ログは時刻同期の仕組みを持たせた上で常時収集するフォレンジックスサーバの設置を行うこと。設定等のログの書込み権限は制限すること。 ログは2箇所以上に記録を実施し、改ざん等の発見を行うこと。 電子署名等による改ざん防止の対策を実施すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				11) 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での証拠として使用するために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のアクセスログ、通信ログは時刻同期の仕組みを持たせた上で常時収集するフォレンジックスサーバの設置を行うこと。設定等のログの書込み権限は制限すること。 ログは2箇所以上に記録を実施し、改ざん等の発見を行うこと。 電子署名等による改ざん防止の対策を実施すること。	
				12) ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のアクセスログ、通信ログは時刻同期の仕組みを持たせた上で常時収集するフォレンジックスサーバの設置を行うこと。設定等のログの書込み権限は制限すること。 ログは2箇所以上に記録を実施し、改ざん等の発見を行うこと。 電子署名等による改ざん防止の対策を実施すること。	
				13) セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理さ	8.1.3	×		
				14) 事件・事故管理手順では、身分が明らかで、認可された要員だけに、作動中のシステム及びデータに対するアクセスを、許すことを考慮す	8.1.3	×		
				15) 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること	8.1.3	×		
				16) 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること	8.1.3	×		
				17) 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認することを考慮すること	8.1.3	×		
			4) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又は実行の分離を考慮すること	1) 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による監督といった他の管理策を考慮すること	8.1.4	×		
				2) セキュリティ監査は、独立性を維持すること	8.1.4	×		
				3) どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること	8.1.4	×		
				4) ある作業を始めることと、その作業を認可することとを分離すること	8.1.4	×		
				5) 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること	8.1.4	×		
				6) 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること	8.1.4	×		
			5) 開発施設、試験施設及び運用施設を分離するため、ソフトウェアの開発から運用の段階への移行についての規則を明確に定め、文書化するこ	1) 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること	8.1.5	×		
				2) 同様な分離は、開発と試験との機能間でも実行すること	8.1.5	×		
				3) 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持す	8.1.5	×		
				4) 開発施設、試験施設及び運用施設を分離すること	8.1.5	×		
				5) 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること	8.1.5	×		
				6) 開発作業と試験作業とは、可能な限り分離すること	8.1.5	×		
				7) コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと	8.1.5	×		
				8) 運用システム及び試験システムに対しては、異なるログオン手順を用	8.1.5	×		
				9) 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること	8.1.5	×		
				10) メニューには、適切な識別メッセージを表示すること	8.1.5	×		
				11) 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得す	8.1.5	×		
				12) 管理用パスワードは、使用後には変更されることを確実にすること	8.1.5	×		
			6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れること	1) 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること	8.1.6	×		
				2) 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること	8.1.6	×		
				3) 外部委託による施設管理においては、事業継続計画との関連性を考	8.1.6	×		
				4) 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮する	8.1.6	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当	8.1.6	×		
				6) 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順	8.1.6	×		
6.2	システムの計画作成及び受入れ	システム故障のリスクを最小限に抑えるため	1) 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること	1) 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること	8.2.1	○	ネットワークトラフィックはサービスを提供するサーバの処理性能、レンタルマシンの設置台数等から余裕を持たせた設計とすること。 増設に当っては、サービス停止時間を極力無くす為、機器の追加のみで設定変更を極力不要とするようなスケールアウト手法による増設が可能な設計を実施すること。 さらにトラフィック量などは常時監視し、統計分析することで、将来的な設備増設計画に反映できること。	・接続サービス：ネットワークトラフィック ・監視サービス：取得するログのディスク容量 等をそれぞれ想定している。
				2) 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資源の使用を監視すること	8.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のシステム資源やトラフィック量はの常時監視を実施すること。	接続サービスに関係ない？ 監視サービスにも関係ない？
				3) 管理者は、使用傾向、特に業務用ソフトウェア又は情報システムの管理ツールと関連した傾向を識別すること	8.2.1	○	通信トラフィック量の増加が予測される傾向(例：新情報の公開、発表、プレスリリース、新サービス、新規ユーザ獲得)を識別するため、 統計的な資源消費傾向を分析できるようなツールを準備すること。 さらに顧客業務フローに連動したトラフィック増減の分析を可能とする為に、トラフィック量の、CPU負荷、メモリ使用量の常時監視を実施し、時系列統計分析を実施すること。	
				4) システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を用いること	8.2.1	○	Webサーバへの DoS攻撃、メールサーバへの過剰なメールの送信、探索行為にあたるポートスキャンを受けたことをメモリ使用状況など常時監視機を実施し、パフォーマンス低下の予兆、ピーク時を情報から統計情報を作成する手順、あるいはシステムを有すること。さらに、システムに対するパッチ適用状況の把握を行い、潜在的な脆弱性を管理すること。 また、異常トラフィックを防止する為にIPS、F/W等の設定が動的に制御可能なシステムを導入すること。	
			2) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること	1) 管理者は、新しいシステムを受け入れるための要求事項及び基準を明確に定義すること	8.2.2	×		
				2) 管理者は、新しいシステムを受け入れるための要求事項及び基準を文書化すること	8.2.2	×		
				3) 管理者は、新しいシステムを受け入れるための要求事項及び基準を合意すること	8.2.2	×		
				4) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な評価を実施すること	8.2.2	×		
				5) 管理者は、新しいシステムを受け入れるための要求事項及び基準を、評価することを確実にすること	8.2.2	×		
				6) システムの受け入れにおいて、性能及びコンピュータの容量・能力の要求事項を考慮すること	8.2.2	×		
				7) システムの受け入れにおいて、誤りからの回復及び再起動の手順並びに障害対策計画を考慮すること	8.2.2	×		
				8) システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮すること	8.2.2	×		
				9) システムの受け入れにおいて、合意された適切なセキュリティ管理策を考慮すること	8.2.2	×		
				10) システムの受け入れにおいて、手動による有効な手順を考慮すること	8.2.2	×		
				11) システムの受け入れにおいて、事業継続の取決めを考慮すること	8.2.2	×		
				12) システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること	8.2.2	×		
				13) システムの受け入れにおいて、新しいシステムが組織のセキュリティ全般に及ぼす影響について、検討したという証拠を得ること	8.2.2	×		
				14) システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと	8.2.2	×		
				15) 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと	8.2.2	×		
				16) 主要な新しいシステム開発においては、適切な試験を実施し、すべての受入れ基準が完全に満たされていることを確認すること	8.2.2	×		
6.3	悪意のあるソフトウェアからの保護	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	1) 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと	8.3.1	×		ウィルスについては、原則として、ウィルスチェックサービスの対象範囲とし、今回抽出したサービスでは個別に扱わない。ただし、監視サービスについては、監視用端末自体のウィルスチェックを想定したため、範囲に含んでいる

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること	8.3.1	×		
				3) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクから保護し、どのような保護対策を行うことが望ましいかを示す組織としての個別方針を考慮すること	8.3.1	×		
				4) 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期	8.3.1	×		
				5) 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること	8.3.1	×		
				6) 未承認のファイル又は無認可の変更の存在に対しては、正式に調査	8.3.1	×		
				7) 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること	8.3.1	×		
				8) 電子メールの添付ファイル及びダウンロードしたファイルのすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること	8.3.1	×		
				9) システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること	8.3.1	×		
				10) ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考	8.3.1	×		
				11) ウイルス感染からの回復のための適切な事業継続計画を考慮するこ	8.3.1	×		
				12) 悪意のあるソフトウェアに関するすべての情報を確認すること	8.3.1	×		
				13) 警告情報が正確、かつ、役立つことを確実にするための手順を考慮す	8.3.1	×		
				14) 管理者は、単なるいたずらと真のウイルスとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること	8.3.1	×		
				15) 職員は、単なるいたずらの問題及びそれらを受け取ったときの対応について認識していること	8.3.1	×		
6.4	システムの維持管理 (Housekeeping)	情報処理及び通信サービスの完全性及び可用性を維持するため	1) 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること	1) 災害又は媒体故障が発生した後、極めて重要なすべての業務情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備えること	8.4.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定情報は定められたバックアップ手順に応じて、設定情報変更のタイミング及び定期的なバッチ処理によるバックアップが行われること。バックアップされたデータは、可能であれば、複数場所にコピーして管理し、リスク分散を図ること。	マシンレンタルサービスのバックアップは、レンタル先のクライアントが原則担当すうため、対象外とする。
				2) 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた場所に保管すること	8.4.1	○	バックアップされたデータは、持ち出し可能な記録媒体にも保存し、免震、耐火構造などを採る場所に一括保管されること。可能であれば、複数場所にコピーして管理し、災害に対するリスク分散を図ること。	
				3) 重要な業務用ソフトウェアについては、少なくとも3世代又は3サイクル分のバックアップのための情報を保持すること	8.4.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定情報は、定期的なバックアップとは別に、トポロジ変更、機器追加、設定変更のタイミングにおいては、手動にてバックアップを実施し、少なくとも3世代は保管すること。	
				4) バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施すこと	8.4.1	○	バックアップされたデータは、持ち出し可能な記録媒体にも保存し、免震、耐火構造などを採る場所に一括保管されること。可能であれば、複数場所にコピーして管理し、災害に対するリスク分散を図ること。	
				5) 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること	8.4.1	○	バックアップされたデータは、持ち出し可能な記録媒体にも保存し、免震、耐火構造などを採る別の場所にも一括保管されること。	
				6) 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定しておくこと	8.4.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定しておくこと	技術的検証項目にあらず
				7) バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること	8.4.1	○	バックアップ媒体は、業務規定に則った周期にて定期的にリード・コンペア等のメディアチェックを実施すること。	
				8) 復元手順は、定期的に検査及び試験すること	8.4.1	○	バックアップデータを復元する手順を確認する為の議事環境を準備すること。	技術的検証項目にあらず
			2) 運用担当者は、自分の作業の記録を継続すること	1) 記録には、システムの起動及び終了の時刻を含めること	8.4.1	×		
				2) 記録には、システム誤り及び実施した是正処置を含めること	8.4.2	×		
				3) 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること	8.4.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 記録には、記録の作成者の名前を含めること	8.4.2	×		
			3) 運用担当者の記録は、定期的に独立した検査を受けること	（なし）	8.4.2	×		
			4) 障害については報告を行い、是正処置をとること	1) 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること	8.4.3	×		
				2) 報告された障害の取扱いについては、明確な規定があること	8.4.3	×		
				3) 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと	8.4.3	×		
				4) 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを	8.4.3	×		
6.5	ネットワークの管理	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること	1) ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること	8.5.1	○	ネットワークのセグメント境界には、F/W、IPS等の不正侵入防止機器を設置すること。複数のユーザの共通基盤となる場合、VPN、VLAN等で分離すること。	接続サービスについては、外部および内部のネットワークを想定、また、監視サービスについては、内部ネットワークを想定。
				2) ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にす	8.5.1	○	ネットワークのセグメント境界には、F/W、IPS等の不正侵入防止機器を設置すること。	
				3) ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること	8.5.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の管理者は、ユーザレンタルサーバや監視システムの管理者とは別の作業者とし、別IDを割り振ること。	
				4) 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立す	8.5.1	×		
				5) 公衆ネットワークを通過するデータの機密性及び完全性を保護するため、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理策を確立すること	8.5.1	○	インターネットからの内部ネットワークへの接続に関しては、IPsec等を用いたVPNサービスを提供すること。VPNに用いる共通鍵の更新が必要な場合、定期的な更新を自動にて行う鍵管理サーバの導入すること。	
				6) サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を	8.5.1	○	Firewallのルール、ルータのルール、ユーザアプリケーションで利用するサービス、監視サービスにて用いる通信の設定内容は矛盾がないよう調整を行うこと。	技術的検証項目にあらず
6.6	媒体の取扱い及びセキュリティ	財産に対する損害及び事業活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること	1) 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること	8.6.1	×		
				2) 組織の管理外となる媒体のすべてについて、認可を必要とすること	8.6.1	×		
				3) 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること	8.6.1	×		
				4) すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること	8.6.1	×		
				5) コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書	8.6.1	×		
			2) 媒体が不要となった場合は、安全、かつ、確実に	1) 媒体の安全な処分のための、正式な手順を確立すること	8.6.1	×		
				2) 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること	8.6.2	×		
				3) 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること	8.6.2	×		
				4) 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと	8.6.2	×		
				5) 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること	8.6.2	×		
				6) 処分しようとする媒体を集める場合、集積することによる影響に配慮	8.6.2	×		
			3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	1) 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類	8.6.3	×		
				2) 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること	8.6.3	×		
				3) 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮	8.6.3	×		
				4) 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持につい	8.6.3	×		
				5) 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを	8.6.3	×		
				6) 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること	8.6.3	×		
				7) 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮す	8.6.3	×		
				8) 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること	8.6.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				9) 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて	8.6.3	×		
				10) 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること	8.6.3	×		
			4) 認可されていないアクセスからシステムに関する文書を保護すること	1) システムに関する文書は、安全に保管すること	8.6.4	×		
				2) システムに関する文書にアクセスできる者は、人数を最小限に抑えるこ	8.6.4	×		
				3) システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること	8.6.4	×		
				4) システムに関する文書で、公衆ネットワークの公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること	8.6.4	×		
6.7	情報及びソフトウェアの交換	組織間で交換される情報の紛失、改ざん又は誤用を防止するため	1) 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと	1) 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること	8.7.1	×		
				2) セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること	8.7.1	×		
				3) セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること	8.7.1	×		
				4) セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術基準標準を考慮するこ	8.7.1	×		
				5) セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること	8.7.1	×		
				6) セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること	8.7.1	×		
				7) セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考	8.7.1	×		
				8) セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考	8.7.1	×		
				9) セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考慮すること	8.7.1	○	コンテンツの授受やアクセスログの統計データなどは標準に従って行うこと。（例：CD-Rへの記録などはISOXXXXの規格） ファイルの形式、暗号化は交換者間で合意されたフォーマットに準拠したソフトウェアなどを利用すること。	
				10) セキュリティ条件にかかわる合意では、取扱いに慎重を要するもの（例えば、暗号かぎ）を保護するために必要とされる特別な管理等を考慮	8.7.1	×		
			2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること	1) 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること	8.7.2	×		
				2) 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いるこ	8.7.2	×		
				3) 媒体の配送においては、宅配業者の身分を確認する手順を導入する	8.7.2	×		
				4) 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること	8.7.2	×		
				5) 媒体の配送においては、施錠されたコンテナの使用を考慮すること	8.7.2	×		
				6) 媒体の配送においては、手渡しを考慮すること	8.7.2	×		
				7) 媒体の配送においては、開封防止包装の利用を考慮すること	8.7.2	×		
				8) 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること	8.7.2	×		
				9) 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること	8.7.2	×		
			3) 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること	1) 電子商取引のセキュリティにおいては、認証（買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求す	8.7.3	×		
				2) 電子商取引のセキュリティにおいては、認可（価格を決める権限、重要な取引文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか、取引相手はこれらをどう	8.7.3	×		
				3) 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること	8.7.3	×		
				4) 電子商取引のセキュリティにおいては、価格情報について考慮すること	8.7.3	×		
				5) 電子商取引のセキュリティにおいては、注文取引について考慮すること	8.7.3	×		
				6) 電子商取引のセキュリティにおいては、審査について考慮すること	8.7.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				7) 電子商取引のセキュリティにおいては、決済について考慮すること	8.7.3	×		
				8) 電子商取引のセキュリティにおいては、注文について考慮すること	8.7.3	×		
				9) 電子商取引のセキュリティにおいては、責任について考慮すること	8.7.3	×		
				10) 電子商取引に関する当事者間の合意は、権限の詳細も含め、合意した取引条件を両当事者に義務付ける契約書によって裏付けること	8.7.3	×		
				11) 情報サービス事業者と付加価値ネットワーク事業者との間にも、合意を交わすこと	8.7.3	×		
				12) 公開している取引システムでは、その取引条件を顧客に公表すること	8.7.3	×		
				13) 電子商取引に用いる基幹コンピュータのもつ攻撃に対する耐性について、及び電子商取引の実施に必要なネットワーク相互接続のセキュリティ上のかかわりについて、	8.7.3	×		
			4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること	1) 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること	8.7.4.1	×		マシンレンタルサービスは、貸し出しサーバ上でクライアントが電子メールを利用する場合を想定。
				2) 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること	8.7.4.2	×		監視サービスについては、障害発生等の連絡を対象となる担当者へ連絡する際に電子メールを使用することを想定。
				3) 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること	8.7.4.2	×		
				4) 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の	8.7.4.2	×		
				5) 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること	8.7.4.2	×		
				6) 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること	8.7.4.2	×		
				7) 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること	8.7.4.2	×		
			5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入	1) 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける情報のぜい(脆)弱性を考慮すること	8.7.5	×		電子オフィスシステムは、監視サービスにおける定期レポート作成の際に使用することを想定。
				2) 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること	8.7.5	×		
				3) 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること	8.7.5	×		
				4) 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること	8.7.5	×		
				5) 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについて	8.7.5	×		
				6) 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮す	8.7.5	×		
				7) 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること	8.7.5	×		
				8) 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること	8.7.5	×		
				9) 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること	8.7.5	×		
				10) 電子オフィスシステムのセキュリティにおいては、緊急時に用いる代替手段についての要求事項及び取決めについて考慮すること	8.7.5	×		
			6) 電子的に公開した情報の完全性を保護するように注意すること	1) 公開されたシステム（例えば、インターネット経由でアクセスできるウェブサーバ）に掲載している情報は、システムが設置された地域又は取引が行われている地域に適用される、法律、規則及び規制に適合する	8.7.5	×		
				2) 情報を公開する前に、正式な認可の手続がとられること	8.7.6	×		
				3) 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって	8.7.6	×		
				4) 公開している電子システムは、それが情報のフィードバック及び直接入力を許すものである場合には、情報は、あらゆるデータ保護に関連して制定された法律に従って収集するこ	8.7.6	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること	8.7.6	×		
				6) 取扱いに慎重を要する情報は、収集の過程及び保管時に保護すること	8.7.6	×		
				7) 公開のシステムにアクセスができても、アクセス権限がないと先のネットワークへのアクセスは、許さないこと	8.7.6	×		
			7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な	1) 音声・画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること	8.7.7	×		
				2) 電話を使うときには、適切な注意を払うことの必要を、職員に意識させること	8.7.7	×		
				3) 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせ	8.7.7	×		
				4) 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残	8.7.7	×		
				5) 職員に、ファクシミリを用いる上での問題点を意識させること	8.7.7	×		
7.1	アクセス制御に関する業務上の	情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定	1) 利用者ごと、または利用者からなるグループごとに対するアクセス制御	9.1.1.1	×		
				2) 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること	9.1.1.1	×		
				3) 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること	9.1.1.1	×		
				4) アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること	9.1.1.1	×		
				5) アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること	9.1.1.1	×		
				6) アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮する	9.1.1.1	×		
				7) アクセス制御に関する個別方針には、異なるシステム及びネットワークにおける、アクセス制御と情報分類の方針との整合性を考慮すること	9.1.1.1	×		
				8) アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること	9.1.1.1	×		
				9) アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用者のアクセス権限情報を考慮すること	9.1.1.1	×		
				10) アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること	9.1.1.1	×		
				11) アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別す	9.1.1.2	×		
				12) アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定すること	9.1.1.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定を行う権限を持つユーザやデータの取り出しを行う運用者、システム設定の管理を行う者などユーザを新たに作成する場合は、デフォルトは全ての権限を制限する設定とし、人為的に設定を変更して権限を与える運用とすること。	
				13) アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をすること	9.1.1.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定を行う権限を持つユーザやデータの取り出しを行う運用者、システム設定の管理を行う者などユーザを新たに作成する場合は、デフォルトは全ての権限を制限する設定とし、人為的に設定を変更して権限を与える運用とすること。	
				14) アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス権の変更をすること	9.1.1.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定を行う権限を持つユーザやデータの取り出しを行う運用者、システム設定の管理を行う者などユーザを新たに作成する場合は、デフォルトは全ての権限を制限する設定とし、人為的に設定を変更して権限を与える運用とすること。	
				15) アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をする	9.1.1.2	×		
7.2	利用者のアクセス管理	情報システムへの認可されていないアクセスを防止するため	1) 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること	1) 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること	9.2.1	×		
				2) 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者IDを用いること	9.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更に対しては担当者毎にIDを割り振ること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 利用者登録手続において、グループIDの使用は、実施される作業に適切な場合にだけ許可すること	9.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更に対しては基本的にはグループIDによる権限は持たせない。	
				4) 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査するこ	9.2.1	×		
				5) 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査するこ	9.2.1	×		
				6) 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査すること	9.2.1	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更に対して割り振られる担当者IDは、上記機器類の設定変更のみの権限しか与えない。	
				7) 利用者登録手続において、重複する利用者IDが別の利用者に発行されないことを確実にすること	9.2.1	○	ユーザIDは社員番号などを用い、過去にさかのぼって一意に割り振られること。	
				8) 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めることを考慮す	9.2.1	×		
				9) 利用者登録手続において、アクセス権の宣言書を利用者に発行するこ	9.2.1	×		
				10) 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること	9.2.1	×		
				11) 利用者登録手続において、認可手続が完了するまでサービス提供者が利用者にアクセスさせないように	9.2.1	×		
				12) 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること	9.2.1	×		
				13) 利用者登録手続において、職務を変更した利用者、又は組織から離れた利用者のアクセス権を直ちに取り消すこと	9.2.1	×		
				14) 利用者登録手続において、もはや必要のない利用者ID及びアカウントがないか定期的に検査し、あれば削除すること	9.2.1	×		
			2) 特権の割り当て及び使用は、制限し、管理すること	1) 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割当てを管理すること	9.2.2	×		
				2) 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別	9.2.2	×		
				3) 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること	9.2.2	×		
				4) 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと	9.2.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更に対して割り振られる担当者IDは、上記機器類の設定変更のみの権限しか与えない。よって、特権の割り当ては、新たに割り振る別IDに付与する運用とする。	技術的検証項目にあらず
				5) 特権の割り当てにおいて、利用者に対する特権の許可が必要ないように、システムルーチンの開発及び使用を促進すること	9.2.2	×		
				6) 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者IDとは別の利用者IDに、割り当てること	9.2.2	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更に対して割り振られる担当者IDは、上記機器類の設定変更のみの権限しか与えない。よって、特権の割り当ては、新たに割り振る別IDに付与する運用とする。	
			3) パスワードの割当ては、正規の管理手続によって統制すること	1) パスワード管理手続の取組において、個人のパスワードを秘密に保つこと	9.2.3	×		
				2) パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に	9.2.3	×		
				3) パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること	9.2.3	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類のOS、アプリケーションに仮パスワード発行機能があるものを採用し、設定を行うこと。	
				4) パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること	9.2.3	×		
				5) パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること	9.2.3	×		
				6) パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避け	9.2.3	×		
				7) パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること	9.2.3	×		
				8) パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと	9.2.3	○	サーバ上にパスワード情報を管理する場合には暗号化を行い、パスワードファイルへのアクセスを制限すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				9) パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びICカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮	9.2.3	○	F/W、ルータ等のネットワーク機器、サービスを提供するDNSサーバ、MAILサーバ等の装置類の設定変更を行う作業に対して、可能であれば、ユーザ認証システムを介した認証手続きとし、可能であればユーザ認証システムに対する認証には個人特定に有効な生体認証方式を用いること。	
			4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること	1) 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと	9.2.4	×		
				2) 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと	9.2.4	×		
				3) 利用者アクセス権の見直しにおいて、特権の割当てを定期的に検査して、認可されていない特権が取得されてないことを確実にすること	9.2.4	×		
7.3	利用者の責任	認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	1) すべての利用者に、パスワードを秘密にしておくように助言すること	9.3.1	×		
				2) すべての利用者に、パスワードを紙に記録して保管しないように助言すること	9.3.1	×		
				3) すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合は、パスワードを変更するように助言すること	9.3.1	×		
				4) すべての利用者に、最短6文字の質の良いパスワードを選択すること	9.3.1	×		
				5) すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること	9.3.1	×		
				6) すべての利用者に、特権アカウントのパスワードは、通常のパスワードより頻繁に変更するように助言する	9.3.1	×		
				7) すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること	9.3.1	×		
				8) すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること	9.3.1	×		
				9) すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること	9.3.1	×		
				10) すべての利用者に、個人用のパスワードを共有しないように助言する	9.3.1	×		
				11) すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言	9.3.1	×		
			2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護すること	9.3.2	×		
				2) 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること	9.3.2	×		
				3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言する	9.3.2	×		
				4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	9.3.2	×		
				5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	9.3.2	×		
7.4	ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	9.4.1	×		
				2) ネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること	9.4.1	○	インターネット(E-mail、HTTP、FTP等)の利用に関する個別方針には、接続可能なネットワーク、利用可能なネットワークサービスを記述すること。	技術ではないと思われる。
				3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	9.4.1	○	インターネット(E-mail、HTTP、FTP等)の利用に関する個別方針には、接続可能なネットワーク、利用可能なネットワークサービスの認可手順を記述すること。	技術ではないと思われる。
				4) ネットワークサービスの使用についての個別方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること	9.4.1	○	インターネット(E-mail、HTTP、FTP等)の利用に関する個別方針には、通信を保護するための管理策及び管理手順を記述すること。	技術ではないと思われる。

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	9.4.1	○	インターネット(E-mail、HTTP、FTP等)の利用に関する個別方針は、業務上のアクセス制御ポリシーと整合性が取れていること。	技術ではないと思われる。
			2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止する	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	9.4.2	○	指定された経路以外での接続を拒否するように、顧客LAN～IDCの経路上のF/Wやルータにおいて、不要なルーティングテーブルの削除、パケットフィルタリング等の制御を実施すること。	
				2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	9.4.2	○	顧客LAN～IDCの接続には専用線を用いること。公衆網を利用する場合には、顧客LAN、IDCそれぞれの境界ルータにおいて、専用の電話番号以外への発呼の拒否、専用の電話番号以外からの着呼を拒否するように設定すること。	
				3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること	9.4.2	○	顧客LAN～IDCの経路では、指定されたサーバ、ポートへの接続のみを許可するように、経路上のF/Wやルータでフィルタリングを行うこと。	インターネット接続の場合はクライアントの設定が出てくるので、自動接続というのがあまり当てはまらない。
				4) 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること	9.4.2	○	管理者メニューにおいては、利用者にはPOPやプロキシのパスワード変更機能、顧客管理者にはメールアドレスの追加、変更機能など必要最低限の機能のみ提供するように制限を設けること。	接続サービスでのメニュー選択となると管理者メニュー<らいしか当てはまらないと思い、管理者メニューに限定して書きました。
				5) 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること	9.4.2	○	顧客LAN～IDCの経路では、指定されたサーバ、ポートへの接続のみ許可するように、経路上のF/Wやルータでフィルタリングを行うこと。	
				6) 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること	9.4.2	○	指定されたサーバ、ポートへの接続のみ許可するように、経路上のF/Wやルータでフィルタリングを行うこと。	
				7) 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること	9.4.2	○	指定されたサーバ、ポートへの接続のみ許可するように、経路上のF/Wやルータでフィルタリングを行うこと。	
				8) 組織内の利用者グループのために別々の論理領域[例えば、仮想私設網（Virtual Private Network：VPN）]を設定することによって、ネットワークアクセスを制限すること	9.4.2	○	利用者の組織内で、グループによるアクセス先のネットワークや利用可能なネットワークサービスの制御を可能とするような仕組みを設けておくこと。	
				9) 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと	9.4.2	×		
			3) 遠隔地からの利用者のアクセスには、認証を行うこと	1) コールバックの手順及び制御を用いるとき、組織は、転送機能をもつネットワークサービスを用いないこと	9.4.3	○	F/Wやルータ、DNSサーバやMAILサーバのリモートメンテナンスにRASを利用する場合で、コールバックの手順及び制御を用いるときには、転送機能をもつサービスを採用しないこと。	
				2) 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること	9.4.3	○	F/Wやルータ、DNSサーバやMAILサーバのリモートメンテナンスにRASを利用する場合で、コールバックの手順及び制御を用いるときには、転送機能を無効にすること。	
				3) コールバックの手順及び制御を徹底的に試験すること	9.4.3	×		
			4) 遠隔コンピュータシステムへの接続は、認証されること	（なし）	9.4.4	○		サブコントロールがない
			5) 診断ポートへのアクセスは、セキュリティを保つように制御されること	1) 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること	9.4.5	○	F/Wやルータ、DNSサーバやMAILサーバのシリアルコンソールには、通常のログイン時と同等の認証を設けること。また、運用オペレータによる操作は、事前に認可された要員が取り決めた手順でのみアクセス可能とするように、適切な保護策を設けること。	
				2) ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にする	9.4.5	×		
			6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること	1) 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること	9.4.6	○	顧客LAN～IDCの経路上のF/Wやルータにおいて、パケットフィルタリングを実施し、要件外の通信は全て遮断するように構成すること。	
				2) ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと	9.4.6	×		
				3) 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮する	9.4.6	×		
			7) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと	1) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること	9.4.7	○	利用者からの認可されていない接続に対する防御策は、業務要件、顧客からの要求事項に従って維持及び更新されること。	技術ではないと思われる。
				2) 電子メールには制限を適用すること	9.4.7	○	MAILサーバにおいては、メールサイズ、MAXホップ数、添付ファイル拡張子等の制限を設けられるようにすること。	
				3) 一方向のファイル転送には制限を適用すること	9.4.7	○	インターネット接続(FTP、HTTP等)のファイルダウンロードには、ファイルサイズ、拡張子などの制限を設けられるようにすること。	
				4) 双方向のファイル転送には制限を適用すること	9.4.7	○	インターネット接続(FTP、HTTP等)のファイルアップロードには、ファイルサイズ、拡張子などの制限を設けられるようにすること。	
				5) 対話型アクセスには制限を適用すること	9.4.7	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログインについては、利用者からのログインは禁止すること。また、運用者のログインも必要最低限に制限すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) 時間帯又は日付に対応したネットワークアクセスには制限を適用すること	9.4.7	○	インターネット(E-mail、HTTP、FTP等)の利用については、利用者の要望に応じ、接続可能な日時、時間帯を制限する機能を設けること。	
			8) 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと	1) 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること	9.4.8	○	指定された経路以外での接続を拒否するように、顧客LAN～IDCの経路上のF/Wやルータにおいて、不要なルーティングテーブルの削除、パケットフィルタリング等の制御を実施すること。	
				2) ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと	9.4.8	×		
			9) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にする	（なし）	9.4.9	×		
7.5	オペレーティングシステムのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること	（なし）	9.5.1	×		
			2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	1) コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時の認証には、IPアドレスや公開鍵による認証等を用い、ID/パスワードによる認証よりも可能な限り強固な方式を採用すること。	
				2) システムについての情報の開示は最小限にすること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時のバナー情報には、システム情報(OS、カーネルバージョン等)を含めないように設定すること。	
				3) ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しないこと	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時のバナー情報や認証エラー時のメッセージには、システム情報(OS、カーネルバージョン等)を含めないように設定すること。	
				4) ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時のバナー情報には、アクセスが認可されている利用者に限定されていることを示す警告を表示すること。	
				5) ログオン手順中に、認可されていない利用者の助けとなる表示をしないこと	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時の認証エラーメッセージには、アカウントの存在確認ができるような情報やシステム情報を表示しないように設定すること。	
				6) 誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しないこと	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時の認証エラーメッセージは、ID、パスワード、IPアドレス等、いずれの認証情報に誤りがあった場合でも同じエラーメッセージを表示すること。	
				7) 許容されるログオンの試みの失敗回数を制限すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログインにおいては、パスワード総当り攻撃や推測攻撃への対策として、連続して認証エラーが発生したアカウントを一時的にロックする機能を設けること。	
				8) ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログインにおいては、パスワード総当り攻撃への対策として、ログイン失敗時に次のログオンの試みが可能となるまでに意図的に時間をおくように設定すること。	
				9) ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、ロックされたアカウントの解除は自動的に行わずに、管理者によるロック解除操作を必要とするように設定すること。	
				10) ログオンの失敗時には、データリンク接続を切ること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、ログイン認証に一定回数連続して失敗した場合にセッションを切断すること。	
				11) ログオン手順のために許容される最長時間及び最短時間を制限すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、ログイン認証に許容する最長時間、最短時間を制限する設定を設けること。	
				12) 許容される最長時間及び最短時間の制限から外れる場合、システムはログオンを終了すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、ログイン認証に許容する最長時間、最短時間の制限を外れた場合に、セッションを切断すること。	
				13) ログオンの失敗時には、失敗した試みを記録すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、ログイン成功時、失敗時のログ(アカウント、IPアドレス、時刻等)を取得すること。	成功時もとったほうが望ましい。
				14) ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログインにおいては、利用者が成りすましに気づく一助とするために、ログイン成功時に前回ログイン日時を表示すること。	
				15) ログオンが無事できた時点で、前回のログオン以降，失敗したログオンの試みがある場合は、その詳細を表示すること	9.5.2	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログインにおいては、利用者が不正ログインの試行に気づく一助とするために、前回ログイン時以降の認証エラーの詳細を表示すること。	
			3) すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ID）を保有	1) 利用者IDには、利用者の特権レベル(例えば、管理者(マネージャ)、監督者(スーパーバイザ)]を表示しないこと	9.5.3	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログインにおいては、利用者の権限(管理者、監督者等)を画面(ターミナル)に表示しないようにすること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 明らかに業務上の利点がある例外的状況において、利用者のグループ又は特定の業務に対して、共有利用者IDを用いる場合、管理者の承認を文書で得ること	9.5.3	×		
			4) 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	1) パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバへのログイン時に利用するパスワードは、管理者による不正を防ぎ、また、責任の所在を明確にするためにも、管理者が付与したパスワードを利用させるのではなく、利用者本人のパスワードを使用させること。	
				2) パスワードの管理システムでは、適切ならば、利用者に自分のパスワードの選択及び変更を許可し、入力誤りを考慮した確認手順を組み入れること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、利用者自身がログインパスワードを変更できるようにパスワード変更機能を提供すること。パスワード変更機能では、現在パスワードと新しいパスワードを2回入力させるようにすること。	
				3) パスワードの管理システムでは、質の良いパスワードを選択させるようにすること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、第三者から推測可能なパスワードをつけられないように、英数字・特殊記号の混在を必須とする、IDと同じパスワードは拒否する等、利用可能なパスワードに一定の制限を設けること。	
				4) パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、定期的にログインパスワードを変更させる機能を設けること。	
				5) パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、仮パスワードを初回ログイン時に変更させる機能を設けること。	
				6) パスワードの管理システムでは、以前の利用者パスワードの記録を、一定期間、維持し再使用を防止すること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、以前に利用者が利用したパスワードを一定期間保持し、再利用を防止する機能を設けること。	
				7) パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにすること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバのパスワード変更機能では、利用者が入力したパスワードを画面上に表示しないようにすること。	
				8) パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバのパスワードファイルは、業務システムのデータとは別に保存すること。	
				9) パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存すること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバのログインパスワードは暗号化してパスワードファイルに保存すること。また、一方向性暗号アルゴリズムを用い、暗号方式を知る管理者でも復元できないようにすること。	
				10) パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること	9.5.4	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、製造者や購入元によって設定されたデフォルトパスワードはすぐに変更すること。	
			5) システムユーティリティのために認証手順を使用すること	1) 業務用ソフトウェアからシステムユーティリティを分離すること	9.5.5	×		
				2) システムユーティリティの使用を、可能な限り少人数の信頼できる認可された利用者だけに制限すること	9.5.5	×		
				3) システムユーティリティを臨時に使用する際には認可をすること	9.5.5	×		
				4) システムユーティリティの使用の制限をすること	9.5.5	×		
				5) システムユーティリティのすべての使用を記録すること	9.5.5	×		
				6) システムユーティリティの認可レベルの明確化及び文書化をすること	9.5.5	×		
				7) すべての不要なユーティリティソフトウェア及びシステムソフトウェアの除去をすること	9.5.5	×		
			6) 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮する	1) 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと	9.5.6	×		
				2) 脅迫に対する警報に対応する責任及び手順を明確に定めること	9.5.6	×		
			7) リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末	1) 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること	9.5.7	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバでは、一定時間入力が無い場合にセッションを無効にするタイムアウト機能を実装すること。	
				2) 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであ	9.5.7	×		
			8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供	1) 既定の時間枠（例えば、バッチファイル伝送のための時間枠）を使うか、又は短時間の通常の対話型処理（session）を用いること	9.5.8	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバの中で特に重要な機器については、ログインを許容する時間を就業時間のみとする等、制限を設けること。	
				2) 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること	9.5.8	○	F/W、ルータ等のネットワーク機器やDNS、MAILサーバの中で、特に重要な機器については、ログインを許容する時間を就業時間のみとする等、制限を設けること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
7.6	業務用ソフトウェアのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	1) 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること	9.6.1	○		
				2) 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮す	9.6.1	○		
				3) 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮	9.6.1	×		
				4) 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること	9.6.1	○		
				5) 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にす	9.6.1	○		
				6) 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること	9.6.1	○		
			2) 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること	1) 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること	9.6.2	×		
				2) 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること	9.6.2	×		
7.7	システムアクセス及びシステム使用状況の監視	認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること	1) 監査記録には、利用者IDを含めること	9.7.1	○		
				2) 監査記録には、ログオン及びログオフの日時を含めること	9.7.1	○		
				3) 監査記録には、可能ならば、端末のID又は所在地を含めること	9.7.1	○		
				4) 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○		
				5) 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○		
			2) 情報処理設備の使用状況を監視する手順を確立すること	1) 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること	9.7.2.1	○		
				2) 監視項目には、認可されているアクセスについて、利用者IDを含むこと	9.7.2.1	○		
				3) 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと	9.7.2.1	○		
				4) 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと	9.7.2.1	○		
				5) 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと	9.7.2.1	○		
				6) 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと	9.7.2.1	○		
				7) 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること	9.7.2.1	○		
				8) 監視項目には、すべての特権操作について、システムの起動及び停止を含めること	9.7.2.1	○		
				9) 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること	9.7.2.1	○		
				10) 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること	9.7.2.1	○		
				11) 監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること	9.7.2.1	○		
				12) 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること	9.7.2.1	×		
				13) 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること	9.7.2.1	○		
				14) 監視項目には、システム警告又は故障について、システム記録例外事項を含めること	9.7.2.1	○		
				15) 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること	9.7.2.1	○		
			3) 監視の結果は、定期的に見直すこと	1) 監視結果の見直しの頻度は、関係するリスクによって決めること	9.7.2.2	×		
				2) 考慮すべきリスク要因には、業務手続に与える重要性の度合を含める	9.7.2.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること	9.7.2.2	×		
				4) 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること	9.7.2.2	×		
				5) 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること	9.7.2.2	×		
			4) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること	1) セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製すること	9.7.2.3	○		
				2) ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮す	9.7.2.3	○		
				3) 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮	9.7.2.3	×		
				4) 記録機能のセキュリティに対して注意すること	9.7.2.3	○		
				5) 管理策は、認可されていない変更及び運用上の問題から保護することを目標とすること	9.7.2.3	○		
			5) コンピュータの時計は正しく設定すること	1) コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時[例えば、万国標準時に（UCT）又は現地の標準時]に合わせること	9.7.3	○		
				2) コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること	9.7.3	○		
7.8	移動型計算処理及び遠隔作業	移動型計算処理及び遠隔作業の設備を用いるときの情報セキュリティを確実にするため	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特	1) 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること	9.8.1	×		
				2) 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること	9.8.1	×		
				3) 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること	9.8.1	×		
				4) 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと	9.8.1	×		
				5) 悪意のあるソフトウェアに対抗する手順を整えること	9.8.1	×		
				6) 悪意のあるソフトウェアに対抗する手順は最新のものであること	9.8.1	×		
				7) 移動型計算処理を用いる要員に対する訓練を計画すること	9.8.1	×		
				8) 情報を素早く、容易にバックアップできる装置が利用可能となっていること	9.8.1	×		
				9) これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること	9.8.1	×		
				10) 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと	9.8.1	×		
				11) ネットワークに接続された移動型設備の使用に対して適切な保護がなされること	9.8.1	×		
				12) 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること	9.8.1	×		
				13) 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること	9.8.1	×		
				14) 大切な、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないこと（可能ならば、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いること）	9.8.1	×		
			2) 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手配されていることを確実にすること	1) 遠隔作業の場所に適切な保護が整っていること	9.8.2	×		
				2) 遠隔作業は、経営陣によって認可され、管理されること	9.8.2	×		
				3) 遠隔作業は、この作業形態のため適切に手配されていること	9.8.2	×		
				4) 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること	9.8.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可	9.8.2	×		
				6) 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮	9.8.2	×		
				7) 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮するこ	9.8.2	×		
				8) 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること	9.8.2	×		
				9) 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること	9.8.2	×		
				10) 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報の取扱いに慎重を要する度合を考慮	9.8.2	×		
				11) 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮	9.8.2	×		
				12) 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの情報又は資源への認可されていないアクセスの脅威を考慮する	9.8.2	×		
				13) 遠隔作業活動のための適切な装置を準備すること	9.8.2	×		
				14) 遠隔作業活動のための適切な保管棚・庫の準備をすること	9.8.2	×		
				15) 遠隔作業活動のための許可される作業を明確にすること	9.8.2	×		
				16) 遠隔作業活動のための作業時間を明確にすること	9.8.2	×		
				17) 遠隔作業活動のための保持してもよい情報の分類を明確にすること	9.8.2	×		
				18) 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること	9.8.2	×		
				19) 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること	9.8.2	×		
				20) 遠隔作業を行う場所の物理的なセキュリティを確保すること	9.8.2	×		
				21) 家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引を明確にすること	9.8.2	×		
				22) ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること	9.8.2	×		
				23) バックアップ及び事業継続のための手順を明確にすること	9.8.2	×		
				24) 監査及びセキュリティの監視を行う	9.8.2	×		
				25) 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること	9.8.2	×		
8.1	システムのセキュリティ要求事項	情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には，管理策についての要求事項を明確にするこ	1) セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること	10.1.1	×		
				2) セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				3) 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考	10.1.1	×		
				4) 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				5) 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること	10.1.1	×		
				6) セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること	10.1.1	×		
				7) セキュリティが確保できなかった場合又はセキュリティが確保されていない場合に起こると思われる業務上の損害の可能性もセキュリティ要求事項及び管理策に反映されるこ	10.1.1	×		
8.2	業務用システムのセキュリティ	業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること	1) 業務取引処理(transaction)、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること	10.2.1	×		
				2) 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				3) データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				4) 入力漏れデータ又は不完全なデータを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				5) データ量の上限及び下限からの超過を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				6) 認可されていない又は一貫しない制御データを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				7) 入力データの妥当性及び完全性を確認するために重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること	10.2.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				8) 入力データに認可されていない変更があるかどうかについての紙に印刷した入力文書の点検を考慮す	10.2.1	×		
				9) 妥当性確認の誤りに対応する手順について考慮すること	10.2.1	×		
				10) 入力データのもっともらしさを試験する手順について考慮すること	10.2.1	×		
				11) データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること	10.2.1	×		
			2) 処理したデータの改変を検出するために，システムに妥当性の検査を組み込むこと	1) 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること	10.2.2.1	×		
				2) データ変更を行う追加・削除の機能を持つプログラムの使用及びその位置について考慮すること	10.2.2.1	×		
				3) プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること	10.2.2.1	×		
				4) データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮	10.2.2.1	×		
				5) 取引処理の更新後のデータファイルのバランスをとるための処理又はバッチの制御を考慮すること	10.2.2.1	×		
				6) 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること	10.2.2.1	×		
				7) システム生成データの妥当性確認を考慮すること	10.2.2.1	×		
				8) 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること	10.2.2.1	×		
				9) レコード及びファイルの全体のハッシュ合計の検査を考慮すること	10.2.2.1	×		
				10) 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること	10.2.2.1	×		
				11) プログラムが正しい順序で実行されることの検査を考慮すること	10.2.2.1	×		
				12) プログラムが正しい順序で実行されない場合は終了され、問題が解決するまでは処理が停止することを確実に実施しているかの検査を考慮	10.2.2.1	×		
			3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮す	1) メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと	10.2.3	×		
			4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をするこ	1) 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと	10.2.4	×		
				2) 出力データの妥当性確認には、すべてのデータの処理を確実にするための調整制御の回数を含むこと	10.2.4	×		
				3) 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、読取り装置又はその後の処理システムにとっての十分な情報の供給を含むこと	10.2.4	×		
				4) 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと	10.2.4	×		
				5) 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと	10.2.4	×		
8.3	暗号による管理策	情報の機密性、真正性又は完全性を保護するため	1) 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること	1) 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること	10.3.1	×		
				2) 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を含めた取組みを、考慮すること	10.3.1	○		
				3) 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを、	10.3.1	○		
				4) 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について、考慮すること	10.3.1	○		
				5) 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について、考慮すること	10.3.1	○		
				6) 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを、考慮すること	10.3.1	○		
				7) 暗号による管理策の使用に関する個別方針を定めるとき、組織全体にわたって効果的に実施するために採用すべき標準類を考慮すること	10.3.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			2) 取扱いに慎重を要する又は重要な情報の機密性を保護するために，暗号化（Encryption）すること	1) リスクアセスメントに基づき，要求される保護レベルを，使用される暗号アルゴリズムの形式及び品質，並びに使用すべき暗号かぎの長さを考慮して明確にすること	10.3.2	○		
				2) 組織における暗号利用の個別方針を実施するとき，世界の異なる地域における暗号技術の使用，及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること	10.3.2	○		
				3) 暗号技術の輸出入に適用される規制も考慮すること	10.3.2	○		
				4) 適切な保護レベルを明らかにするため，及び要求される保護レベルを提供し，かぎ管理機能をもつ安全な製品を選択するために，専門家の助言を求めること	10.3.2	○		
				5) 組織が意図した暗号使用に適用される法令及び規制に関して，必要に応じて法律家の助言を求めること	10.3.2	○		
			3) 電子文書の真正性及び完全性を保護するために，ディジタル署名を用いること	1) 秘密かぎの機密性を保護するために注意を払うこと	10.3.3	×		
				2) 秘密かぎにアクセスした者は，文書に署名でき，その結果かぎの所有者の署名を盗用することがあり得るため，このかぎを秘密に保管するこ	10.3.3	×		
				3) 公開かぎの完全性を保護すること	10.3.3	×		
				4) ディジタル署名に使用される暗号かぎは，暗号化に使用されるものとは異なること	10.3.3	×		
				5) ディジタル署名を用いるときは，ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること	10.3.3	×		
				6) 電子商取引の場合，ディジタル署名の法的位置付けを知ること	10.3.3	×		
				7) 法的枠組みが不十分である場合，ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること	10.3.3	×		
				8) 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては，法律家による助言を求める	10.3.3	×		
			4) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には，否認防止サービスを用いる	（なし）	10.3.4	×		
			5) 一連の合意された標準類，手順及び方法に基づくかぎ管理システムを，暗号技術の利用を支援するために用いること	1) 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること	10.3.5.1	○		
				2) すべてのかぎは，変更及び破壊から保護し，共通かぎ及び秘密かぎは，認可されていない露呈から保護	10.3.5.1	○		
				3) かぎを生成し，保存し，記録保管するために用いられる装置を保護するためには，物理的保護策を用いるこ	10.3.5.1	○		
				4) かぎ管理システムでは，種々の暗号システム及び種々の業務用ソフトウェアのためのかぎを生成する方法を定めること	10.3.5.1	○		
				5) かぎ管理システムでは，公開かぎ証明書を生成し入手する方法を定めること	10.3.5.1	○		
				6) かぎ管理システムでは，予定している利用者にかぎを配付する方法を定めること	10.3.5.2	○		
				7) かぎ管理システムでは，かぎを保存する方法を定めること	10.3.5.2	○		
				8) かぎ管理システムでは，かぎを変更又は更新する方法を定めること	10.3.5.2	○		
				9) かぎ管理システムでは，セキュリティが損なわれたかぎを処理する方法について定めること	10.3.5.2	○		
				10) かぎ管理システムでは，かぎを無効にする方法について定めること	10.3.5.2	○		
				11) かぎ管理システムでは，事業継続管理の一部として，例えば，暗号化された情報の回復のために，消失したかぎ又は損傷したかぎを回復する方法を定めること	10.3.5.2	○		
				12) かぎ管理システムでは，かぎを，例えば，記録保管された情報又はバックアップされた情報などのために，記録保管する方法について定める	10.3.5.2	○		
				13) かぎ管理システムでは，かぎを破壊する方法を定めること	10.3.5.2	○		
				14) かぎ管理システムでは，かぎ管理に関連する活動を記録し監査する方法を定めること	10.3.5.2	○		
				15) かぎ管理システムでは，セキュリティが損なわれる可能性を軽減するために，かぎは一定期間だけ用いることができるように，かぎの活性化及び非活性化の期日を定めるこ	10.3.5.2	○		
				16) かぎの活性化及び非活性化の期間は，暗号による管理策が使用される環境及び認識されているリスクによって決めること	10.3.5.2	○		
				17) 安全に管理された共通かぎ及び秘密かぎの問題に加え，公開かぎの保護についても考慮すること	10.3.5.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				18) 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に	10.3.5.2	×		
8.4	システムファイルのセキュリティ	ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にする	1) 運用システムでのソフトウェアの実行を管理すること	1) 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること	10.4.1	○		
				2) 運用システムは、実行可能なコードだけを保持すること	10.4.1	○		
				3) 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れの確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しな	10.4.1	○		
				4) 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること	10.4.1	○		
				5) 古い版のソフトウェアは、事故対策用として保持すること	10.4.1	○		
				6) 運用システムに使用されるベンダー供給ソフトウェアは、供給者によって支援されるレベルで、維持管理され	10.4.1	○		
				7) 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること	10.4.1	○		
				8) セキュリティ上の欠陥を除去するか又は軽減するのに役立つ場合には、ソフトウェアパッチを適用するこ	10.4.1	○		
				9) 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること	10.4.1	○		
				10) 供給者の活動は監視されることが望ましい	10.4.1	○		
			2) 試験データを保護し，管理すること	1) システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと	10.4.2	○		
				2) 個人情報が入っている運用データベースは、使用しないようにすること	10.4.2	○		
				3) 個人情報が入っている情報を使用する場合は，使用する前に，個人的要素を消去すること	10.4.2	○		
				4) 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用	10.4.2	○		
				5) 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けるこ	10.4.2	○		
				6) 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること	10.4.2	○		
				7) 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること	10.4.2	○		
			3) プログラムソースライブラリへのアクセスに対しては，厳しい管理を維持す	1) 可能な限り、プログラムソースライブラリは、運用システムに含めないこと	10.4.3	×		
				2) 各アプリケーションごとに、プログラムライブラリ管理責任者を任命する	10.4.3	×		
				3) IT支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと	10.4.3	×		
				4) 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと	10.4.3	×		
				5) その業務用ソフトウェアのためのIT支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プログラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること	10.4.3	×		
				6) プログラムリストは、セキュリティの保たれた環境に保持されること	10.4.3	×		
				7) プログラムソースライブラリへのすべてのアクセスについて、監査記録を維持管理すること	10.4.3	×		
				8) ソースプログラムの旧版は、記録保管しておくこと	10.4.3	×		
				9) 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと	10.4.3	×		
				10) プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従うこと	10.4.3	×		
8.5	開発及び支援過程におけるセキュリティ	業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理すること	1) 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないこと	10.5.1	○		
				2) 支援プログラマによるシステムへのアクセスはその作業に必要な部分に限定されること	10.5.1	○		
				3) 変更に対する正式な合意及び承認が得られていることを確実にするこ	10.5.1	○		
				4) 業務用ソフトウェア及び運用の変更管理手順は統合されること	10.5.1	○		
				5) 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること	10.5.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確実にすること	10.5.1	○		
				7) 業務用ソフトウェア及び運用の変更過程では、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするためにこの手順をレビューすること	10.5.1	○		
				8) 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識	10.5.1	○		
				9) 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を	10.5.1	○		
				10) 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること	10.5.1	○		
				11) 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること	10.5.1	○		
				12) 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新されること	10.5.1	○		
				13) 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実に	10.5.1	○		
				14) 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェアの更新について版数の管理を行うこと	10.5.1	○		
				15) 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること	10.5.1	○		
				16) 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること	10.5.1	○		
				17) 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること	10.5.1	○		
			2) オペレーティングシステムを変更した場合は，業務用システムをレビューし，試験すること	1) オペレーティングシステムの変更によって業務用ソフトウェアの管理及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること	10.5.2	×		
				2) 年間支援計画及び予算には、オペレーティングシステムの変更の結果として必要となるレビュー及びシステム試験を必ず含めるようにするこ	10.5.2	×		
				3) 実施前に行う適切なレビューに間に合うように、オペレーティングシステムの変更を通知することを確実にす	10.5.2	×		
				4) 事業継続計画に対して適切な変更がなされることを確実にすること	10.5.2	×		
			3) パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更を厳しく管理すること	1) ベンダー供給のパッケージソフトウェアは、変更しないで使用すること	10.5.3	×		
				2) パッケージソフトウェアの変更が絶対必要であると判断された場合は、組み込まれている管理策及び完全性の処理が損なわれるリスクを考	10.5.3	×		
				3) パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること	10.5.3	×		
				4) パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる可能性を考慮すること	10.5.3	×		
				5) パッケージソフトウェアの変更が絶対必要であると判断された場合は、変更の結果として、将来のソフトウェア保守に対して組織が責任を負うようになるかどうかの影響を考慮	10.5.3	×		
				6) 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと	10.5.3	×		
				7) 変更はすべて、完全に試験すること	10.5.3	×		
				8) 変更はすべて、文書化すること	10.5.3	×		
				9) 将来更新されたソフトウェアに再び適用できるようにすること	10.5.3	×		
			4) 隠れチャネル（Covert channels）及びトロイの木馬（Trojan code）の危険性から保護するために，ソフトウェアの購入，使用及び修正を管理し，検査すること	1) プログラムは定評のある開発元のものだけを購入すること	10.5.4	○		
				2) コードの確認ができるようにソースコードでプログラムを購入すること	10.5.4	○		
				3) 評価された製品を用いること	10.5.4	○		
				4) 使用前にすべてのソースコードを検査すること	10.5.4	○		
				5) 一旦導入したコードへのアクセス及びそのコードへの変更を管理するこ	10.5.4	○		
				6) 重要なシステムでの作業には確実に信頼できる要員を用いること	10.5.4	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために，管理策を用いること	1) ソフトウェア開発を外部委託する場合、使用許諾に関する取決め、コードの所有権及び知的所有権について考慮すること	10.5.5	×		
				2) ソフトウェア開発を外部委託する場合、実施される作業の質及び正確さの認証を考慮すること	10.5.5	×		
				3) ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託（escrow）契約に関する取決めについて考慮すること	10.5.5	×		
				4) ソフトウェア開発を外部委託する場合、なされた作業の質及び正確さの監査のためのアクセス権について考慮すること	10.5.5	×		
				5) ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること	10.5.5	×		
				6) ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること	10.5.5	×		
9.1	事業継続管理の種々の面	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため	1) 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること	1) 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること	11.1.1	×		
				2) 業務手続の中断が事業に及ぼすと思われる影響を理解し（組織の存続性を脅かす可能性のある重大な事件・事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である）、情報処理施設の事業目的を確立すること	11.1.1	×		
				3) 事業継続の手続の一部をなすこともある適切な保険への加入を考慮	11.1.1	×		
				4) 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること	11.1.1	×		
				5) 合意された戦略に従って事業継続計画を明確にし、文書化すること	11.1.1	×		
				6) 実行されている計画及び手続を定期的に試験し、更新すること	11.1.1	×		
				7) 事業継続管理が組織の手続及び機構に確実に組み込まれるようにする	11.1.1	×		
				8) 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること	11.1.1	×		
			2) 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること	1) それらの障害の影響（損害規模及び回復期間の両面から）を判断するために、リスクアセスメントを行うこと	11.1.2	×		
				2) これら両活動の実施には、事業資源及び手続の管理者が全面的に関与すること	11.1.2	×		
			3) 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てること	1) 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること	11.1.2	×		
			4) 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること	1) 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること	11.1.3	×		
				2) 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施す	11.1.3	×		
				3) 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に注意すること	11.1.3	×		
				4) 事業継続計画の作成過程では、合意された手順及び過程を文書化す	11.1.3	×		
				5) 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと	11.1.3	×		
				6) 事業継続計画の作成過程では、計画の試験及び更新を行うこと	11.1.3	×		
				7) 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと	11.1.3	×		
				8) これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること	11.1.3	×		
			5) すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること	1) 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること	11.1.4	×		
				2) 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正す	11.1.4	×		
				3) 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件を考慮すること	11.1.4	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 事業継続計画作成の枠組みでは、事業運営及び/又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること	11.1.4	×		
				5) 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決めを含むこと	11.1.4	×		
				6) 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の手順について考慮すること	11.1.4	×		
				7) 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること	11.1.4	×		
				8) 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表について考慮すること	11.1.4	×		
				9) 事業継続計画作成の枠組みでは、事業継続手続を理解させ、手続が継続して有効であることを確保するために計画される認識及び教育活動について考慮すること	11.1.4	×		
				10) 事業継続計画作成の枠組みでは、個人の責任について考慮すること	11.1.4	×		
				11) 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するのに誰が責任をもつかを記述すること	11.1.4	×		
				12) 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること	11.1.4	×		
				13) 事業継続計画作成の枠組みでは、各計画には特定の責任者がいるこ	11.1.4	×		
				14) 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること	11.1.4	×		
				15) 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者の責任とすること	11.1.4	×		
			6) 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること	1) 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職員がそれらの計画を確実に認識するものであること	11.1.5.1	×		
				2) 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと	11.1.5.1	×		
				3) 計画の個々の構成要素を、頻繁に試験すること	11.1.5.1	×		
				4) 計画が実際に役立つことを保証するために、様々な手法を使用するこ	11.1.5.1	×		
				5) 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画の検討）	11.1.5.1	×		
				6) 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）	11.1.5.1	×		
				7) 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）	11.1.5.1	×		
				8) 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施す	11.1.5.1	×		
				9) 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）	11.1.5.1	×		
				10) 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験す	11.1.5.1	×		
				11) いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反映させること	11.1.5.1	×		
			7) 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること	1) 事業継続上の問題を適切に対処することを確実にするための手順は、組織の変更管理プログラムの中に含まれること	11.1.5.2	×		
				2) 各事業継続計画の定期的見直しに対する責任を割り当てること	11.1.5.2	×		
				3) 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に更新すること	11.1.5.2	×		
				4) この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること	11.1.5.2	×		
10.1	法的要求事項への適合	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避ける	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項に適合する特定の管理策、及び個々の責任も同様に明確に定め、文書化すること	12.1.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は，法的制限事項に適合するように，適切な手続を実行す	1) ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること	12.1.2.2	×		
				2) ソフトウェア製品の取得手続に関する標準類を発行すること	12.1.2.2	×		
				3) ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること	12.1.2.2	×		
				4) 適切な財産登録簿を維持管理すること	12.1.2.2	×		
				5) 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること	12.1.2.2	×		
				6) 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること	12.1.2.2	×		
				7) 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確認すること	12.1.2.2	×		
				8) 適切な使用許諾条件を維持管理するための個別方針を定めること	12.1.2.2	×		
				9) ソフトウェアの処分又は他人への譲渡についての個別方針を定めること	12.1.2.2	×		
				10) 適切な監査ツールを用いること	12.1.2.2	×		
				11) 公衆ネットワークから入手するソフトウェア及び情報の使用条件に従うこ	12.1.2.2	×		
			3) 組織の重要な記録は、消失、破壊及び改ざんから保護されること	1) 記録類は、記録の種類（例えば、会計記録、データベース記録、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について保持期間及び記録媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光学媒体）の詳細も定めておく	12.1.3	×		
				2) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること	12.1.3	×		
				3) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、必要なときに、認可されている者が使用できるようにすること	12.1.3	×		
				4) 記録の保管に用いられる媒体が劣化する可能性を考慮すること	12.1.3	×		
				5) 保管及び取扱いの手順は、製造業者の推奨に従って実行すること	12.1.3	×		
				6) 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確保する手順を	12.1.3	×		
				7) 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式で取り出すことができるように、データ保管システムを選択すること	12.1.3	×		
				8) 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にす	12.1.3	×		
				9) 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること	12.1.3	×		
				10) 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行す	12.1.3	×		
				11) 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること	12.1.3	×		
				12) 主要な情報の出典一覧を維持管理すること	12.1.3	×		
				13) 重要な記録及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実行すること	12.1.3	○ ﾈｯﾄﾜｰｸﾛｸﾞ		
			4) 関連する法令に従って個人情報を保護するために，管理策を用いること	1) データ保護の担当責任者を任命すること	12.1.4	×		
				2) 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当責任者に報告することは、データ所有者の責任であること	12.1.4	×		
				3) 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任で	12.1.4	×		
			5) 情報処理施設の使用には管理者の認可を要するものとし，そのような施設の誤用を防ぐための管理策を用いること	1) 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされること	12.1.5	×		
				2) 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること	12.1.5	×		
				3) 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること	12.1.5	×		
				4) すべての利用者は、その許可されたアクセスの正確な範囲を認識していること	12.1.5	×		
				5) 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを通知すること	12.1.5	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	インターネット接続サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告メッセージをコンピュータの画面上に表	12.1.5	○		
				7) 利用者は、引き続きログオン処理を行うために画面上のメッセージに同意し、それに適切に対応すること	12.1.5	×		
			6) 暗号による管理策の策定においては、国の法律への適合を確実なものにするために，法的な助言を求めること	1) 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること	12.1.6	×		
			7) 人又は組織に対する措置を支援するには，十分な証拠をもつこと	1) 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること	12.1.7.1	×		
				2) 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとる	12.1.7.1	×		
				3) 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること	12.1.7.3	×		
				4) コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっ	12.1.7.3	○		
				5) コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること	12.1.7.3	×		
				6) コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること	12.1.7.3	×		
				7) 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得る	12.1.7.3	×		
10.2	セキュリティ基本方針及び技術適合のレビュー	組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため	1) 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること	1) 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること	12.2.1	×		
				2) 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること	12.2.1	×		
			2) 情報システムは，セキュリティ実行標準と適合していることを定期的に検査すること	1) 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行	12.2.2	○		
				2) 技術適合の検査では、専門家の技術援助を得ること	12.2.2	×		
				3) 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアによって実施されるこ	12.2.2	○		
				4) 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること	12.2.2	×		
				5) いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施さ	12.2.2	×		
10.3	システム監査の考慮事項	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意され	1) 監査要求事項は、担当経営陣の同意を得ること	12.3.1	×		
				2) 検査の範囲は、合意され、管理されること	12.3.1	×		
				3) 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定するこ	12.3.1	×		
				4) 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること	12.3.1	×		
				5) 複製ファイルは、監査が完了した時点で消去すること	12.3.1	×		
				6) 検査を実施するための情報資源は、明確に識別され、利用可能であ	12.3.1	×		
				7) 特別又は追加処理の要求事項は、識別され、合意されること	12.3.1	×		
				8) すべてのアクセスは、照合用の証跡を残すために、監視され、記録さ	12.3.1	×		
				9) すべての手順、要求事項及び責任について、文書化すること	12.3.1	×		
			2) システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること	1) システム監査ツールは、開発及び運用システムから分離しておくこと	12.3.2	×		
				2) システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと	12.3.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
5.2	装置のセキュリティ	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	1) 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置し又は保護すること	1) 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること	7.2.1	○	監視装置はラックに収納すること。収納したラック内には、関連する機器のみを収納すること。ラックは施錠しておくこと。 監視端末を設置する作業区域には、関連する機器のみを設置すること。この作業区域は、他の作業と共用しないこと。また、通路から容易に侵入できないようにすること。	ここでは、各サービスにおける次の装置等を想定する。
				2) 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること	7.2.1	○	監視装置の保守時に使用する表示画面、および、監視端末の表示画面は、関係者以外の者が、操作者の肩越しに覗き見ることのできない位置、角度になっていること。	・マシンレンタルサービス：レンタル用サーバおよび通信機器。
				3) 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること	7.2.1	○	監視装置または監視端末のセキュリティレベルが他の機器よりも高い場合は、設置する区画を、レベルの高い区画として分離すること。	・接続サービス：インターネット接続に必要な、FWサーバおよびルータ等の通信機器。
				4) 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の策定を考慮すること	7.2.1	×		・監視サービス：監視用の端末等
				5) 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること	7.2.1	○	監視装置および監視端末の設置場所、同一階の設置場所周辺、及び設置場所の上下階の周辺に関して、温度、湿度、浮遊粒子、塵埃、漏水、火気、消火設備、騒音、振動、悪臭等の状況が、監視装置及びその操作者に悪影響を及ぼさないこと。また、これらを発生させる可能性についても考慮すること。	・ファシリティ：入退館管理装置、監視カメラ等
				6) 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること	7.2.1	○	監視装置の保守時に使用するキーボードの表面、または、監視端末のキーボードの表面等に、塵埃の著しい付着が認められる場合には、キーボードカバー等を使用す	
				7) 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること	7.2.1	×		
			2) 装置は、停電、その他の電源異常から保護するこ	1) 装置は、装置製造者の仕様に適合した適切な電力の供給を確保する	7.2.2	×		
				2) 電源の多重化をすること	7.2.2	×		
				3) 無停電電源装置（UPS）を設置する	7.2.2	×		
				4) 非常用発電機の設置をすること	7.2.2	×		
				5) 障害対策計画では、UPSが故障した場合に取るべき措置についても計画しておくこと	7.2.2	×		
				6) UPSは、容量が十分であることを定期的に確認すること	7.2.2	×		
				7) UPSは、製造者の推奨に従って点検すること	7.2.2	×		
				8) 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること	7.2.2	×		
				9) 発電機を使用する場合、製造者の推奨に従って定期的に点検すること	7.2.2	×		
				10) 発電機を長時間運転できるように、燃料の十分な供給を確保すること	7.2.2	×		
				11) 電源の緊急スイッチは、機械室の非常口近くに設置すること	7.2.2	×		
				12) 主電源の停電時用として非常用照明を備えること	7.2.2	×		
				13) 落雷防護はすべての建物に備えること	7.2.2	×		
				14) すべての外部通信回線に落雷防護フィルタを付けること	7.2.2	×		
			3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受又は損傷から保護するこ	1) 情報処理設備に接続する電源ケーブル及び通信回線は、可能ならば地下に埋設するか、又はそれに代わる十分な保護手段を施すこと	7.2.3	×		
				2) ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること	7.2.3	○	監視装置と監視対象を接続するネットワーク、及び、監視端末と監視装置を接続するネットワークのケーブル配線の経路は、ラックの内部、床下のフリーアクセスフロア、床上のモール、天井裏のキャットウォーク、フロアのパイプスペース等を利用すること。ラック、パイプスペース等、アクセスが容易な部分には施錠すること。ケーブルの露出を最小限にすること。	ネットワークケーブルに関する管理は、各サービスに付随するハードウェアの一部として、各サービス毎に掘り下げる。
				3) 干渉を防止するために、電源ケーブルは通信ケーブルから隔離すること	7.2.3	○	監視装置、及び、監視端末において、電源ケーブルと通信ケーブルは、別区分とし、お互いを30cm以上の間隔を空けて布設すること。交差させるときは、交差角度を直角にすること。電磁干渉（EMI）が残る場合は、金属板、金網、金属箔等により、電磁遮蔽すること。	
				4) 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること	7.2.3	○	監視装置と監視対象を接続するネットワークケーブルが、外部に露出していて断線や盗聴の恐れが特に高い場合は、外装電線管を導入すること。	
				5) 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること	7.2.3	○	監視装置と監視対象を接続するネットワーク、及び、監視端末と監視装置を接続するネットワークの点検箇所、終端箇所については、施錠可能な部屋、場所、ラック、ボックス内に設置すること。	
				6) 取扱いに慎重を要するシステム又は重要なシステムに対しては、代替経路又は伝送媒体を使用すること	7.2.3	○	監視サービスが中断したときの影響が特に大きい場合には、ネットワーク配線を二重化すること。	
				7) 取扱に慎重を要するシステム又は重要なシステムに対しては、光ファイバケーブルを使用すること	7.2.3	○	監視装置と監視対象を接続するネットワーク、及び、監視端末と監視装置を接続するネットワークについて、盗聴や電磁干渉（EMI）の恐れが特に高い場合には、光ファイバーケーブルを使用すること。	
				8) 認可されていない装置がケーブルに取り付けられているかどうかについての調査すること	7.2.3	○	監視装置と監視対象を接続する通信ケーブル、及び、監視端末と監視装置を接続する通信ケーブルに、正式に認可されていないハブや盗聴装置が取り付けられていないか、その経路に沿って定期的に目視調査すること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
			4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく実施すること	1) 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること	7.2.4	○	監視装置及び監視端末の保守については、監視装置または監視端末の供給者が推奨する整備間隔がある場合、もしくは仕様書に整備間隔を含む保守についての記載がある場合は、それらに定められたところに従い、定期的な保守を実施すること。	
				2) 認可された保守担当者だけが装置の修理及び手入れを実施すること	7.2.4	○	監視装置及び監視端末に関して、保守契約を締結している場合は、その契約先の保守担当者、保守契約を締結していない場合及び社内で保守を実施している場合は、社内の保守担当者のみが、分解、調整、部品交換、設定変更等の修理を実施すること。操作者は、取扱説明書等で利用者に許可されている範囲内で、機器の操作、利用者交換可能部品の交換、清掃等の運用を実施すること。	
				3) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること	7.2.4	○	監視装置、又は、監視端末に関して、何らかの異常動作、不具合等の障害が発生した場合には、その大小に係わらず、その内容を記録すること。また、障害を予防するために実施した保守、及び、障害を是正するために実施した保守については、その内容を記録すること。	
				4) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること	7.2.4	○	前項の記録については、一定期間、保管すること。	
				5) 装置を保守するために搬出する場合、適切な管理策を施すこと	7.2.4	○	監視装置又は監視端末を保守するために保守委託先に搬出する場合、機器内に残っている監視情報が漏洩するリスク、監視情報が消去されて利用できなくなるリスクを防ぐため、機器内の情報はバックアップを取ってから削除すること。ただし、監視情報が暗号化してあれば、削除は省略してもよい。	
				6) 保険約款によって定められたすべての要求事項に従うこと	7.2.4	×		
			5) 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可	1) 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること	7.2.5	×		接続サービス、監視サービスにおいて、専門家が自宅よりリモート接続して操作することを想定している。
				2) 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと	7.2.5	○	専門家が自宅からリモート接続に使用するノートPCを、自宅外に持ち運ぶ場合は、車上荒らし、置き引き等のリスクから守るため、自動車内、電車の網棚上、飲食店内等に放置しないこと。	
				3) ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること	7.2.5	○	専門家が自宅からリモート接続に使用するノートPCを、自宅外に持ち運ぶ場合は、カバンの中に入れること。ただし、シースルーバッグ、メーカーロゴ付きバッグ、パソコン専用バッグ等、パソコンが中に入っていることを予期させるカバンは避けること。	
				4) 装置の保護に関しては、製造者の指示に常に従うこと	7.2.5	○	取扱説明書等の注意事項を守ること。	
				5) 在宅作業についての管理策は、リスクアセスメントによって決定すること	7.2.5	○	リスクアセスメントにおいて、自宅からリモート接続することを前提として、なりすまし、情報漏えい、外部からの不正アクセス、侵入窃盗（空き巣）、強盗等のリスクを考慮すること。	
				6) 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御策）を適用すること	7.2.5	○	自宅からリモート接続に使用するノートPCには、起動時のパスワードを設定し、スクリーンセーバにパスワード保護を掛けること。仕事に関連する書類は、机上に放置せず、鍵の掛かる引き出し等にしまうこと。	
				7) 事業所外の装置を保護するために、十分な保険が付保されていること	7.2.5	○	自宅における、侵入窃盗（空き巣）及び強盗等、また、自宅外における、置き引き、窃盗、紛失等が、会社又は個人の加入する損害保険の求償範囲に含まれていること。	
				8) セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること	7.2.5	○	自宅からリモート接続に使用するノートPCには、信頼性の低いソフトウェアをインストールしないこと。定期的にスパイウェアを検出可能な検知ソフトウェアを実行すること。インターネットカフェ、無線LANで使用しないこと。	
			6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に上書きすること	1) 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること	7.2.6	○	監視装置、監視端末を処分する場合、次のいずれかによること。 (1) ディスククラッシャー装置を使用して、磁気ディスクを物理的に破壊すること。あるいは、磁気ディスク装置を分解し、内部の磁気ディスク（円板）を、ハンマー、ヤスリ等を使用して破壊すること。磁気ディスクが複数枚ある場合は、すべてに実施すること。 (2) 消磁装置を使用して、磁気ディスク上のデータを消去すること。さらに、データ復元ソフトを使用しても、データが復元できないこと。 (3) データ完全消去ソフトを使用してデータを消去すること（上書き7回以上）。さらに、データ復元ソフトを使用しても、データが復元できないこと。	ファシリティでは、生体認証の情報等を想定している。
				2) 取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアが、消去又は上書きされているか確認	7.2.6	○	（前項に同じ）	
5.3	その他の管理策	情報及び情報処理設備の損傷又は盗難を防止するため	1) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用、並びに情報処理設備に対するクリアスクリーン方針の適用を考慮	1) クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること	7.3.1	×		
				2) クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること	7.3.1	×		
				3) 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管す	7.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				4) 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと	7.3.1	×		
				5) パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと	7.3.1	×		
				6) パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること	7.3.1	×		
				7) 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること	7.3.1	×		
				8) 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと	7.3.1	×		
				9) 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと	7.3.1	×		
			2) 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできな	1) 持出し時及び返却時に記録を残すこと	7.3.2	×		
				2) 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること	7.3.2	×		
				3) 現場検査があることを各人が認識していること	7.3.2	×		
6.1	運用手順及び責任	情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと	1) 操作手順は、正式な文書として取り扱うこと	8.1.1	×		ファシリティでは、入退室管理、各種制御系システムを想定。
				2) 操作手順が変更の場合は管理者によって認可されること	8.1.1	×		
				3) 操作手順には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				4) 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記	8.1.1	×		
				5) 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記	8.1.1	×		
				6) 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				7) 操作手順には、特別な出力の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記す	8.1.1	×		
				8) 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				9) 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること	8.1.1	×		
			2) 情報処理設備及びシステムの変更について管理すること	1) 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること	8.1.2	×		
				2) 運用プログラムは、厳重な変更管理の下に置くこと	8.1.2	○	運用プログラムの変更について、実行者と承認者を分離すること。変更ごとに、変更手順、不具合発生時の復帰手順を明確にし、記録として残すこと。変更前にテストが実行されており、変更後の運用に支障がないことが確認されていること。	
				3) プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること	8.1.2	○	前項の記録に加え、運用プログラムの変更の実施日時、変更内容、変更実施者、動作確認の成否を記録すること。	
				4) 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合すること	8.1.2	×		
				5) 重要な変更を識別及び記録すること	8.1.2	○	緊急性、影響範囲など、重要な変更を識別するための判断基準を作成すること。記録には、重要な変更であるかどうかの識別欄を設け、記入すること。	
				6) 重要な変更の潜在的な影響の評価をすること	8.1.2	×		
				7) 変更の申出を正式に承認する手順を確立すること	8.1.2	×		
				8) 変更の詳細の、全関係者への通知をすること	8.1.2	×		
				9) うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること	8.1.2	×		
			3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任及び手順を確立	1) 情報システムの故障及びサービスの停止に対処できるように、手順を定めること	8.1.3	×		
				2) サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること	8.1.3	×		
				3) 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること	8.1.3	×		
				4) 機密性に対する違反に対処できるように、手順を定めること	8.1.3	×		
				5) 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を含めること	8.1.3	×		
				6) 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること	8.1.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				7) 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること	8.1.3	×		
				8) 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること	8.1.3	×		
				9) 通常の障害対策計画手順には、監督機関に対する措置の報告を含め	8.1.3	×		
				10) 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	×		
				11) 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での証拠として使用するために、監査証跡及びこれに類する証拠を収集し、安全に保管する	8.1.3	○	アクセスログには、次のものを含めること。 ・監視装置、監視端末に対するアクセス時の、ユーザーID、ログイン時刻、ログアウト時刻、アクセス内容（コマンド等） アクセスログは、別のサーバーにコピーを保管するか、媒体に書き出すこと。	
				12) ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	アクセスログには、次のものを含めること。 ・監視装置の稼動状況、監視ログの取得状況、監視ソフトウェアの実行状況 アクセスログは、別のサーバーにコピーを保管するか、媒体に書き出すこと。	
				13) セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理さ	8.1.3	×		
				14) 事件・事故管理手順では、身分が明らかで、認可された要員だけに、作動中のシステム及びデータに対するアクセスを、許すことを考慮す	8.1.3	×		
				15) 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること	8.1.3	×		
				16) 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること	8.1.3	×		
				17) 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認することを考慮すること	8.1.3	×		
			4) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又は実行の分離を考慮す	1) 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による監督といった他の管理策を考慮すること	8.1.4	×		
				2) セキュリティ監査は、独立性を維持すること	8.1.4	×		
				3) どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること	8.1.4	×		
				4) ある作業を始めることと、その作業を認可することとを分離すること	8.1.4	×		
				5) 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること	8.1.4	×		
				6) 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること	8.1.4	×		
			5) 開発施設、試験施設及び運用施設を分離するため、ソフトウェアの開発から運用の段階への移行についての規則を明確に定め、文書化するこ	1) 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること	8.1.5	×		
				2) 同様な分離は、開発と試験との機能間でも実行すること	8.1.5	×		
				3) 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持す	8.1.5	×		
				4) 開発施設、試験施設及び運用施設を分離すること	8.1.5	×		
				5) 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること	8.1.5	×		
				6) 開発作業と試験作業とは、可能な限り分離すること	8.1.5	×		
				7) コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと	8.1.5	×		
				8) 運用システム及び試験システムに対しては、異なるログオン手順を用いること	8.1.5	×		
				9) 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること	8.1.5	×		
				10) メニューには、適切な識別メッセージを表示すること	8.1.5	×		
				11) 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得す	8.1.5	×		
				12) 管理用パスワードは、使用後には変更されることを確実にすること	8.1.5	×		
			6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れ	1) 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること	8.1.6	×		
				2) 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること	8.1.6	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 外部委託による施設管理においては、事業継続計画との関連性を考慮すること	8.1.6	×		
				4) 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮すること	8.1.6	×		
				5) 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当てを考慮すること	8.1.6	×		
				6) 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順を考慮すること	8.1.6	×		
6.2	システムの計画作成及び受入れ	システム故障のリスクを最小限に抑えるため	1) 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容量・能力を予測すること	1) 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること	8.2.1	○	過去数か月分の監視ログ容量、通常時の負荷、繁忙時の負荷、インシデント発生時の負荷、将来予測等のデータを元に、監視端末、監視装置について、その運用期間全体にわたる負荷を予測・算出し、所要容量・能力の予測を行うこと。	・接続サービス：ネットワークトラフィック ・監視サービス：取得するログのディスク容量 等をそれぞれ想定している。
				2) 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資源の使用を監視すること	8.2.1	○	（該当しない） （汎用大型コンピュータは、システム上に存在しない）	
				3) 管理者は、使用傾向、特に業務用ソフトウェア又は情報システムの管理ツールと関連した傾向を識別すること	8.2.1	×		
				4) システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を	8.2.1	×		
			2) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を実施すること	1) 管理者は、新しいシステムを受け入れるための要求事項及び基準を明確に定義すること	8.2.2	×		
				2) 管理者は、新しいシステムを受け入れるための要求事項及び基準を文書化すること	8.2.2	×		
				3) 管理者は、新しいシステムを受け入れるための要求事項及び基準を合意すること	8.2.2	×		
				4) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な評価を実施すること	8.2.2	×		
				5) 管理者は、新しいシステムを受け入れるための要求事項及び基準を、評価することを確実にすること	8.2.2	×		
				6) システムの受け入れにおいて、性能及びコンピュータの容量・能力の要求事項を考慮すること	8.2.2	×		
				7) システムの受け入れにおいて、誤りからの回復及び再起動の手順並びに障害対策計画を考慮すること	8.2.2	×		
				8) システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮すること	8.2.2	×		
				9) システムの受け入れにおいて、合意された適切なセキュリティ管理策を考慮すること	8.2.2	×		
				10) システムの受け入れにおいて、手動による有効な手順を考慮すること	8.2.2	×		
				11) システムの受け入れにおいて、事業継続の取決めを考慮すること	8.2.2	×		
				12) システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること	8.2.2	×		
				13) システムの受け入れにおいて、新しいシステムが組織のセキュリティ全般に及ぼす影響について、検討したという証拠を得ること	8.2.2	×		
				14) システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと	8.2.2	×		
				15) 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと	8.2.2	×		
				16) 主要な新しいシステム開発においては、適切な試験を実施し、すべての受入れ基準が完全に満たされていることを確認すること	8.2.2	×		
6.3	悪意のあるソフトウェアからの保護	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	1) 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと	8.3.1	×		ウィルスについては、原則として、ウィルスチェックサービスの対象範囲とし、今回抽出したサービスでは個別に扱わない。ただし、監視サービスについては、監視用端末自体のウィルスチェックを想定したため、範
				2) ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること	8.3.1	×		
				3) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクから保護し、どのような保護対策を行うことが望ましいかを示す組織としての個別方針を考慮すること	8.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期更新を考慮すること	8.3.1	○	監視端末そのものに対して、ウイルスの検出及び修復の機能を有するウイルス対策ソフトウェアを導入すること。ウイルス定義ファイルは自動アップデート機能等を利用して、定期的に更新すること。ウイルス対策ソフトウェア本体は、ソフトウェアの改訂内容等を考慮して、必要に応じて更新すること。	
				5) 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること	8.3.1	×		
				6) 未承認のファイル又は無認可の変更の存在に対しては、正式に調査すること	8.3.1	○	監視端末上のシステムファイル等に、未承認のものを発見した場合、または、認可されていない変更を発見した場合は、正式に調査を実施すること。	
				7) 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること	8.3.1	○	出所の不明確な電子媒体上のファイル、認可されていない電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、リアルタイムスキャン等の機能により、ファイルを使用する前にウイルス検査を実施すること。	
				8) 電子メールの添付ファイル及びダウンロードしたファイルのすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること	8.3.1	○	電子メールの添付ファイル、及びダウンロードしたファイルのすべてに対し、リアルタイムスキャン等の機能により、ファイルを使用する前に悪意のあるソフトウェアの検査を実施すること。	
				9) システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること	8.3.1	○	システムをウイルスから保護すること。ウイルスから保護する対策の利用方法について、関連する従業者に教育を行うこと。	
				10) ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考慮すること	8.3.1	○	監視端末がウイルスに感染した場合は、決められた手順書に従い、報告し、また、感染からの回復を行うこと。また、複数の人が関わる場合、責任、指示系統が明確であること。	
				11) ウイルス感染からの回復のための適切な事業継続計画を考慮すること	8.3.1	○	事業継続計画で想定する事件・事故の一つとして、ウイルス感染からの回復を含めること。これには、すべての必要なデータ、及びソフトウェアのバックアップからの回復を含めること。	
				12) 悪意のあるソフトウェアに関するすべての情報を確認すること	8.3.1	○	悪意のあるソフトウェアの攻撃を受けた恐れのある場合は、関連するすべての情報を確認し、警告情報が正確で有用であることを確認すること。	
				13) 警告情報が正確、かつ、役立つことを確実にするための手順を考慮す	8.3.1	×		
				14) 管理者は、単なるいたずらと真のウイルスとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること	8.3.1	○	システムの管理者は、警察庁、経済産業省、総務省、IPA/ISEC、JPCERT/CC、セキュリティ情報提供サイト、ウイルス対策ソフト供給元、OS 供給元、アプリケーションソフト供給元等の適切な情報源を予めブラウザに登録しておくこと。単なるいたずらと真のウイルスとを識別するために、これらの情報源の情報を確認すること。	
				15) 職員は、単なるいたずらの問題及びそれらを受け取ったときの対応について認識していること	8.3.1	○	従業者に、単なるいたずらという可能性があることと、いたずらを受け取ったときの対処方法について、教育を実施すること。	
6.4	システムの維持管理 (Housekeeping)	情報処理及び通信サービスの完全性及び可用性を維持するため	1) 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること	1) 災害又は媒体故障が発生した後、極めて重要なすべての業務情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備えること	8.4.1	○	バックアップ事業所として、開発拠点が考えられているが、バックアップ事業所の形態として、ホットサイト、ウォームサイト、コールドサイトのいずれが適しているのか検討すること。また、現状の形態と一致しているか確認すること。バックアップの対象範囲、バックアップ頻度、及びバックアップの方法（差分バックアップ、インクリメンタルバックアップ、フルバックアップ）について決定すること。	マシンレンタルサービスのバックアップは、レンタル先のクライアントが原則担当すうため、対象外とする。
				2) 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた場所に保管すること	8.4.1	○	バックアップ事業所が、主事業所の災害による損傷を免れることができるほど、十分離れた場所にあるかどうか確認すること。最小限のバックアップ情報、バックアップについての正確及び完全な記録、並びに文書化された復元手順を、バックアップ事業所に保管すること。	
				3) 重要な業務用ソフトウェアについては、少なくとも3世代又は3サイクル分のバックアップのための情報を保持すること	8.4.1	○	監視装置で監視するアクセスログ及びアラートについては、少なくとも三か月分の情報を保持すること。監視結果のデータベースについては、少なくとも3世代又は3サイクル分のバックアップ情報を保持すること。	
				4) バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施すこと	8.4.1	○	バックアップされた情報は、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施すこと。	
				5) 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること	8.4.1	○	主事業所において媒体に適用する管理策は、バックアップ事業所における媒体に対しても適用すること。	
				6) 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定しておくこと	8.4.1	○	重要な業務上の情報について、保存期間を決定しておくこと。また、半永久的に保持すべき保管用文書に対する要求事項は、すべて明確にしておくこと。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				7) バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること	8.4.1	○	バックアップした媒体について、現実的に実施可能であれば、定期的に検査を実施すること。検査の実施方法については、ファイルのメタデータ、エラー情報、またはハッシュ値等を利用する、システムコマンド、または検査用ツール等の中から適切な検査手段を選択すること。	
				8) 復元手順は、定期的に検査及び試験すること	8.4.1	○	バックアップした媒体からのデータ復旧手順については、手順が有効であることの確認と、復旧に要する時間が災害復旧計画や事業継続計画で割り当てられた時間内に完了することの確認のために、定期的に試験を実施すること。試験の実施方法については、チェックリスト試験、構造化ウォークスルー試験、シミュレーション試験、並行運用試験、完全中断試験等の中から適切な試験形態と実施頻度を決めること。	
			2) 運用担当者は、自分の作業の記録を継続するこ	1) 記録には、システムの起動及び終了の時刻を含めること	8.4.1	×		
				2) 記録には、システム誤り及び実施した是正処置を含めること	8.4.2	×		
				3) 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること	8.4.2	×		
				4) 記録には、記録の作成者の名前を含めること	8.4.2	×		
			3) 運用担当者の記録は、定期的に独立した検査を受けること	（なし）	8.4.2	×		
			4) 障害については報告を行い、是正処置をとること	1) 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること	8.4.3	×		
				2) 報告された障害の取扱いについては、明確な規定があること	8.4.3	×		
				3) 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと	8.4.3	×		
				4) 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを	8.4.3	×		
6.5	ネットワークの管理	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること	1) ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること	8.5.1	○	ネットワークの管理者は、監視対象の内部ネットワークと、監視側の内部ネットワークのそれぞれについて、機密性、完全性、可用性の観点からネットワーク上のデータのセキュリティが確保されているか、検討すること。	接続サービスについては、外部および内部のネットワークを想定、また、監視サービスについては、内部ネットワークを想定。
				2) ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること	8.5.1	○	監視装置においては、監視マネージャ機能等のサービスが、監視端末以外の端末から利用できないようにすること。 監視端末においては、ネットワークに対するサービスは停止すること。	
				3) ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること	8.5.1	○	次の者は兼任しないようにすること。 (1) ネットワーク管理者と、監視装置の操作者 (2) ネットワーク管理者と、監視端末の操作者	
				4) 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立す	8.5.1	×		
				5) 公衆ネットワークを通過するデータの機密性及び完全性を保護するため、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理策を確立すること	8.5.1	×		
				6) サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整すること	8.5.1	○	様々な管理活動は、次の二つの理由のため、綿密に調整した上で実施すること。 (1) 提供するサービスを事業目的に合致した最適なものにするため (2) 管理策が情報処理基盤全体に一様に適用されることを確実にするため	
6.6	媒体の取扱い及びセキュリティ	財産に対する損害及び事業活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること	1) 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること	8.6.1	×		
				2) 組織の管理外となる媒体のすべてについて、認可を必要とすること	8.6.1	×		
				3) 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること	8.6.1	×		
				4) すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること	8.6.1	×		
				5) コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書化すること	8.6.1	×		
			2) 媒体が不要となった場合は、安全、かつ、確実に処分すること	1) 媒体の安全な処分のための、正式な手順を確立すること	8.6.1	×		
				2) 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること	8.6.2	×		
				3) 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること	8.6.2	×		
				4) 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと	8.6.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること	8.6.2	×		
				6) 処分しようとする媒体を集める場合、集積することによる影響に配慮すること	8.6.2	×		
			3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	1) 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類に対応させて策定すること	8.6.3	×		
				2) 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること	8.6.3	×		
				3) 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮すること	8.6.3	×		
				4) 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持について考慮すること	8.6.3	×		
				5) 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを確実にすること	8.6.3	×		
				6) 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること	8.6.3	×		
				7) 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮す	8.6.3	×		
				8) 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること	8.6.3	×		
				9) 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて考慮すること	8.6.3	×		
				10) 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること	8.6.3	×		
			4) 認可されていないアクセスからシステムに関する文書を保護すること	1) システムに関する文書は、安全に保管すること	8.6.4	×		
				2) システムに関する文書にアクセスできる者は、人数を最小限に抑えるこ	8.6.4	×		
				3) システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること	8.6.4	×		
				4) システムに関する文書で、公衆ネットワークの公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること	8.6.4	×		
6.7	情報及びソフトウェアの交換	組織間で交換される情報の紛失、改ざん又は誤用を防止するため	1) 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと	1) 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること	8.7.1	×		
				2) セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること	8.7.1	×		
				3) セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること	8.7.1	×		
				4) セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術基準標準を考慮するこ	8.7.1	×		
				5) セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること	8.7.1	×		
				6) セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること	8.7.1	×		
				7) セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考	8.7.1	×		
				8) セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考	8.7.1	×		
				9) セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考慮すること	8.7.1	○	・ログを収集、分析しているか ・ログの改ざんを抑止する施策を講じているか ・ログは一定期間保管しているか ・ログを収集するシステムは時刻同期をとっているか	ログデータ
				10) セキュリティ条件にかかわる合意では、取扱いに慎重を要するもの（例えば、暗号かぎ）を保護するために必要とされる特別な管理策を考慮	8.7.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること	1) 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること	8.7.2	×		
				2) 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いること	8.7.2	×		
				3) 媒体の配送においては、宅配業者の身分を確認する手順を導入すること	8.7.2	×		
				4) 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること	8.7.2	×		
				5) 媒体の配送においては、施錠されたコンテナの使用を考慮すること	8.7.2	×		
				6) 媒体の配送においては、手渡しを考慮すること	8.7.2	×		
				7) 媒体の配送においては、開封防止包装の利用を考慮すること	8.7.2	×		
				8) 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること	8.7.2	×		
				9) 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること	8.7.2	×		
			3) 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること	1) 電子商取引のセキュリティにおいては、認証（買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求すべきか）について考慮すること	8.7.3	×		
				2) 電子商取引のセキュリティにおいては、認可（価格を決める権限、重要な取引文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか、取引相手はこれらをどうやって知るか）について考慮すること	8.7.3	×		
				3) 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること	8.7.3	×		
				4) 電子商取引のセキュリティにおいては、価格情報について考慮すること	8.7.3	×		
				5) 電子商取引のセキュリティにおいては、注文取引について考慮すること	8.7.3	×		
				6) 電子商取引のセキュリティにおいては、審査について考慮すること	8.7.3	×		
				7) 電子商取引のセキュリティにおいては、決済について考慮すること	8.7.3	×		
				8) 電子商取引のセキュリティにおいては、注文について考慮すること	8.7.3	×		
				9) 電子商取引のセキュリティにおいては、責任について考慮すること	8.7.3	×		
				10) 電子商取引に関する当事者間の合意は、権限の詳細も含め、合意した取引条件を両当事者に義務付ける契約書によって裏付けること	8.7.3	×		
				11) 情報サービス事業者と付加価値ネットワーク事業者との間にも、合意を交わすこと	8.7.3	×		
				12) 公開している取引システムでは、その取引条件を顧客に公表すること	8.7.3	×		
				13) 電子商取引に用いる基幹コンピュータのもつ攻撃に対する耐性について、及び電子商取引の実施に必要なネットワーク相互接続のセキュリティ上のかかわりについて、	8.7.3	×		
			4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮すること	1) 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること	8.7.4.1	○	・メールサーバにウィルス対策ソフトを導入しているか ・電子メールソフトウェアは限定されているか ・電子メールソフトウェアは最新バージョンになっているか ・電子メールソフトウェアのパスワードを設定しているか ・電子メールのパスワードを保存していないか	電子メールの保護
				2) 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること	8.7.4.2	○	・顧客の機密情報を電子メールに添付して送信していないか ・電子メールにファイルを添付して送信する場合は、当該添付ファイルに暗号化やパスワードを付しているか	添付ファイルの暗号化
				3) 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること	8.7.4.2	×		
				4) 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の責任を含めること	8.7.4.2	×		
				5) 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること	8.7.4.2	○	・機密性の高い情報の送信時にはＳＳＬ通信等、暗号化しているか	ＳＳＬ通信
				6) 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること	8.7.4.2	○	・業務上、送受信したメールは、一定期間保管しているか	メールの保管
				7) 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること	8.7.4.2	○	・メールを閲覧し管理しているか （送信の成功／失敗や送信先等の管理）	メールの管理
			5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針及び手引を作成し、導入	1) 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける情報のぜい(脆)弱性を考慮すること	8.7.5	○	・サーバのパッチやウィルス対策ソフトを最新バージョンの更新を適宜行っているか	サーバのセキュリティ
				2) 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること	8.7.5	○	・情報の機密性に基づいて共用する/共用しないを決定しているか ・共用する情報については、業務上の必要性等からアクセス権限を付与する者を決定しているか	共用ファイルのアクセス権限

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること	8.7.5	×		
				4) 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること	8.7.5	○	・機密性の高い情報については、権限の有する者のみアクセスできるよう制御しているか	アクセス制御
				5) 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについて考慮すること	8.7.5	○	・ＯＳやネットワークソフトのメーカーサポートは継続されているか ・ＯＳやネットワークソフトは、業務処理の重要性に応じたセキュリティ機能を備えているか	ソフトウェアのサポートや機能性
				6) 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮す	8.7.5	○	・職員、請負業者等に分けてアクセスできる設備を決定しているか	設備のアクセス制御
				7) 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること	8.7.5	○	・サーバルーム等、重要な設備やエリアへのアクセスは、業務上必要な者に限定しているか	サーバルームへのアクセス
				8) 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること	8.7.5	○	・利用者のアクセス権限は、業務上必要な最小限の権限を設定しているか	利用者権限
				9) 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること	8.7.5	○	・サーバのバックアップを採取しているか ・バックアップは必要な期間保管しているか	バックアップ
				10) 電子オフィスシステムのセキュリティにおいては、緊急時に用いる代替手段についての要求事項及び取決めについて考慮すること	8.7.5	○	・障害発生時、復旧のための手順を確立しているか	リカバリ手順
			6) 電子的に公開した情報の完全性を保護するように注意すること	1) 公開されたシステム（例えば、インターネット経由でアクセスできるウェブサーバ）に掲載している情報は、システムが設置された地域又は取引が行われている地域に適用される、法律、規則及び規制に適合することを確実にすること	8.7.5	×		
				2) 情報を公開する前に、正式な認可の手続がとられること	8.7.6	×		
				3) 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって	8.7.6	×		
				4) 公開している電子システムは、それが情報のフィードバック及び直接入力を許すものである場合には、情報は、あらゆるデータ保護に関連して制定された法律に従って収集するこ	8.7.6	×		
				5) 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること	8.7.6	×		
				6) 取扱いに慎重を要する情報は、収集の過程及び保管時に保護するこ	8.7.6	×		
				7) 公開のシステムにアクセスができても、アクセス権限がないと先のネットワークへのアクセスは、許さないこ	8.7.6	×		
			7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な手順及び管理策をもつこ	1) 音声・画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること	8.7.7	×		
				2) 電話を使うときには、適切な注意を払うことの必要を、職員に意識させること	8.7.7	×		
				3) 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせ	8.7.7	×		
				4) 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残さないようにさせること	8.7.7	×		
				5) 職員に、ファクシミリを用いる上での問題点を意識させること	8.7.7	×		
7.1	アクセス制御に関する業務上の要求事項	情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定義し、文書化すること	1) 利用者ごと、または利用者からなるグループごとに対するアクセス制御規則を、アクセス方針宣言書に明確に記述すること	9.1.1.1	×		
				2) 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること	9.1.1.1	×		
				3) 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること	9.1.1.1	×		
				4) アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること	9.1.1.1	×		
				5) アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること	9.1.1.1	×		
				6) アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮する	9.1.1.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				7) アクセス制御に関する個別方針には、異なるシステム及びネットワークにおける、アクセス制御と情報分類の方針との整合性を考慮すること	9.1.1.1	×		
				8) アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること	9.1.1.1	×		
				9) アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用者のアクセス権限情報を考慮すること	9.1.1.1	×		
				10) アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること	9.1.1.1	×		
				11) アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別す	9.1.1.2	×		
				12) アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定す	9.1.1.2	○	・アクセス権限は、原則「アクセス不可」とし、許可された者のみ「アクセス可能」なルールとしているか	アクセス制御ルール
				13) アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をするこ	9.1.1.2	○	・アクセス権限を定期的に見直しているか	アクセス権の見直し
				14) アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス権の変更をすること	9.1.1.2	○	・管理者によって、利用者のアクセス権は業務上必要な権限が付与されているかが管理されているか	アクセス権の変更
				15) アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をする	9.1.1.2	×		
7.2	利用者のアクセス管理	情報システムへの認可されていないアクセスを防止するため	1) 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること	1) 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること	9.2.1	×		
				2) 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者IDを用いること	9.2.1	○	・利用者IDは、個人ごとに付与されているか	個別ID
				3) 利用者登録手続において、グループIDの使用は、実施される作業に適切な場合にだけ許可すること	9.2.1	○	・共用IDは、必要な場合に限定して付与されているか	共用ID
				4) 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査するこ	9.2.1	×		
				5) 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査するこ	9.2.1	×		
				6) 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査するこ	9.2.1	○	・利用者IDに付与された権限は、業務上必要な権限に限定されているか	ID権限
				7) 利用者登録手続において、重複する利用者IDが別の利用者に発行されないことを確実にすること	9.2.1	○	・利用者IDの重複を避ける手段を講じているか	
				8) 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めることを考慮す	9.2.1	×		
				9) 利用者登録手続において、アクセス権の宣言書を利用者に発行するこ	9.2.1	×		
				10) 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること	9.2.1	×		
				11) 利用者登録手続において、認可手続が完了するまでサービス提供者が利用者にアクセスさせないように	9.2.1	×		
				12) 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること	9.2.1	×		
				13) 利用者登録手続において、職務を変更した利用者、又は組織から離れた利用者のアクセス権を直ちに取り消すこと	9.2.1	×		
				14) 利用者登録手続において、もはや必要のない利用者ID及びアカウントがないか定期的に検査し、あれば削除すること	9.2.1	×		
			2) 特権の割り当て及び使用は、制限し、管理すること	1) 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割当てを管理すること	9.2.2	×		
				2) 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別	9.2.2	×		
				3) 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること	9.2.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				4) 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと	9.2.2	○	・特権IDは、認可手続が完了するまで、許可しないような制限ができているか	特権IDの使用可能時期
				5) 特権の割り当てにおいて、利用者に対する特権の許可が必要ないように、システムルーチンの開発及び使用を促進すること	9.2.2	×		
				6) 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者IDとは別の利用者IDに、割り当て	9.2.2	○	・特権IDは、通常の業務用途に使用される利用者IDとは別の利用者IDを割当てているか	特権IDの割当
			3) パスワードの割当ては、正規の管理手続によって統制すること	1) パスワード管理手続の取組において、個人のパスワードを秘密に保つこと	9.2.3	×		
				2) パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に	9.2.3	×		
				3) パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること	9.2.3	○	・パスワードの付与において、最初にログオンする際に変更が強制されるパスワードが最初に発行されるようなしくみになっているか	初期パスワードの強制変更
				4) パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること	9.2.3	×		
				5) パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること	9.2.3	×		
				6) パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避け	9.2.3	×		
				7) パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること	9.2.3	×		
				8) パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと	9.2.3	○	・パスワードリストをパスワード保護や暗号化等をせずに保存していないか	パスワードリストの保護
				9) パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びICカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮	9.2.3	○	・重要なシステムには、ID／パスワード以外の個人認証も用いているか	他の個人認証の併用
			4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること	1) 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと	9.2.4	×		
				2) 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと	9.2.4	×		
				3) 利用者アクセス権の見直しにおいて、特権の割当てを定期的に検査して、認可されていない特権が取得されてないことを確実にすること	9.2.4	×		
7.3	利用者の責任	認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	1) すべての利用者に、パスワードを秘密にしておくように助言すること	9.3.1	×		
				2) すべての利用者に、パスワードを紙に記録して保管しないように助言すること	9.3.1	×		
				3) すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合は、パスワードを変更するように助言すること	9.3.1	×		
				4) すべての利用者に、最短6文字の質の良いパスワードを選択すること	9.3.1	×		
				5) すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること	9.3.1	×		
				6) すべての利用者に、特権アカウントのパスワードは、通常のパスワードより頻繁に変更するように助言する	9.3.1	×		
				7) すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること	9.3.1	×		
				8) すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること	9.3.1	×		
				9) すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること	9.3.1	×		
				10) すべての利用者に、個人用のパスワードを共有しないように助言する	9.3.1	×		
				11) すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言	9.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
			2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護すること	9.3.2	×		
				2) 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること	9.3.2	×		
				3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言する	9.3.2	×		
				4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	9.3.2	×		
				5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	9.3.2	×		
7.4	ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	9.4.1	×		
				2) ネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること	9.4.1	×		技術検証項目ではない
				3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	9.4.1	×		技術検証項目ではない
				4) ネットワークサービスの使用についての個別方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること	9.4.1	×		技術検証項目ではない
				5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	9.4.1	×		技術検証項目ではない
			2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止する	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	9.4.2	○	・利用できるネットワーク経路を限定しているか	ネットワーク経路の限定
				2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	9.4.2	○	・限定したネットワーク経路を盗聴等を防止するために専用線等で保護しているか	ネットワーク経路の保護
				3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続す	9.4.2	○	・ファイアウォールを設置しているか	ファイアウォール
				4) 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること	9.4.2	○	・利用者が利用できるネットワーク機能等を限定しているか	利用機能の限定
				5) 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること	9.4.2	○	・ネットワークの探索ができる範囲を制限しているか	ネットワークの探索
				6) 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること	9.4.2	○	・外部ネットワークを利用する際には、ファイアウォールを必ず通過するようなネットワーク構成になっているか ・外部のネットワークからの攻撃を防御するため、ファイアウォールで社内ネットワークを保護するネットワーク構成になっているか	ファイアウォールでの攻撃防御
				7) 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること	9.4.2	○	・社内外の通信をファイアウォールのログを収集し分析しているか	通信の監視
				8) 組織内の利用者グループのために別々の論理領域[例えば、仮想私設網（Virtual Private Network：VPN）]を設定することによって、ネットワークアクセスを制限すること	9.4.2	○	・重要な拠点同士の通信には、VPN等アクセスを制限する施策を施しているか	VPN
				9) 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと	9.4.2	×		
			3) 遠隔地からの利用者のアクセスには、認証を行うこと	1) コールバックの手順及び制御を用いるとき、組織は、転送機能をもつネットワークサービスを用いないこと	9.4.3	○	・遠隔地アクセスでの認証は、転送機能を利用していないか	転送機能の利用禁止
				2) 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること	9.4.3	○		
				3) コールバックの手順及び制御を徹底的に試験すること	9.4.3	×		
			4) 遠隔コンピュータシステムへの接続は、認証されること	（なし）	9.4.4	○	・遠隔地アクセスは個人認証及び端末認証を用いているか	遠隔地アクセスの認証
			5) 診断ポートへのアクセスは、セキュリティを保つように制御されること	1) 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること	9.4.5	○	・診断ポートへは、管理者以外の者がアクセスできないよう制限されているか	診断ポートの利用制限

項番	項目	目的	コントロール	サブコントロール	JIS X 5080:2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				2) ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にする	9.4.5	×		
			6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること	1) 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること	9.4.6	○	・ファイアウォールは、認められた通信やアクセスのみを行えるよう設定されているか	ファオアウォールの設定
				2) ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと	9.4.6	×		
				3) 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮する	9.4.6	×		
			7) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと	1) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること	9.4.7	×		
				2) 電子メールには制限を適用すること	9.4.7	○	・電子メール機能は、業務必要な者以外は利用を制限しているか	メールの制限
				3) 一方向のファイル転送には制限を適用すること	9.4.7	○	・ファイル転送機能やプロトコルは、業務上必要なもの以外を制限しているか	ファイル転送機能等の制限
				4) 双方向のファイル転送には制限を適用すること	9.4.7	○		
				5) 対話型アクセスには制限を適用すること	9.4.7	○		
				6) 時間帯又は日付に対応したネットワークアクセスには制限を適用する	9.4.7	○	・アクセスできる日（平日のみ等）や時間帯（9：00～20：00まで等）を制限しているか	アクセス可能時間・日の限定
			8) 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと	1) 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること	9.4.8	○	・ファイアウォールやルーターにより、外部のネットワークからの侵入を防げるようなルーティング機能をもっているか	ルーティング
				2) ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと	9.4.8	×		
			9) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にする	（なし）	9.4.9	×		
7.5	オペレーティングシステムのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること	（なし）	9.5.1	×		
			2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	1) コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること	9.5.2	○		
				2) システムについての情報の開示は最小限にすること	9.5.2	○		
				3) ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しな	9.5.2	○		
				4) ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示するこ	9.5.2	○		
				5) ログオン手順中に、認可されていない利用者の助けとなる表示をしない	9.5.2	○		
				6) 誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しないこ	9.5.2	○		
				7) 許容されるログオンの試みの失敗回数を制限すること	9.5.2	○		
				8) ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと	9.5.2	○		
				9) ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること	9.5.2	○		
				10) ログオンの失敗時には、データリンク接続を切ること	9.5.2	○		
				11) ログオン手順のために許容される最長時間及び最短時間を制限する	9.5.2	○		
				12) 許容される最長時間及び最短時間の制限から外れる場合、システムはログオンを終了すること	9.5.2	○		
				13) ログオンの失敗時には、失敗した試みを記録すること	9.5.2	○		
				14) ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること	9.5.2	○		
				15) ログオンが無事できた時点で、前回のログオン以降、失敗したログオンの試みがある場合は、その詳細を表示すること	9.5.2	○		
			3) すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ID）を保有	1) 利用者IDには、利用者の特権レベル[例えば、管理者(マネージャ)、監督者(スーパーバイザ)]を表示しないこと	9.5.3	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 明らかに業務上の利点がある例外的状況において、利用者のグループ又は特定の業務に対して、共有利用者IDを用いる場合、管理者の承認を文書で得ること	9.5.3	×		
			4) 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	1) パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること	9.5.4	○		
				2) パスワードの管理システムでは、適切ならば、利用者に自分のパスワードの選択及び変更を許可し、入力誤りを考慮した確認手順を組み	9.5.4	○		
				3) パスワードの管理システムでは、質の良いパスワードを選択させるようにすること	9.5.4	○		
				4) パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること	9.5.4	○		
				5) パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること	9.5.4	○		
				6) パスワードの管理システムでは、以前の利用者パスワードの記録を、一定期間、維持し再使用を防止す	9.5.4	○		
				7) パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにすること	9.5.4	○		
				8) パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること	9.5.4	○		
				9) パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存す	9.5.4	○		
				10) パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること	9.5.4	○		
			5) システムユーティリティのために認証手順を使用すること	1) 業務用ソフトウェアからシステムユーティリティを分離すること	9.5.5	×		
				2) システムユーティリティの使用を、可能な限り少人数の信頼できる認可された利用者だけに制限すること	9.5.5	×		
				3) システムユーティリティを臨時に使用する際には認可をすること	9.5.5	×		
				4) システムユーティリティの使用の制限をすること	9.5.5	×		
				5) システムユーティリティのすべての使用を記録すること	9.5.5	×		
				6) システムユーティリティの認可レベルの明確化及び文書化をすること	9.5.5	×		
				7) すべての不要なユーティリティソフトウェア及びシステムソフトウェアの除去をすること	9.5.5	×		
			6) 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮する	1) 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと	9.5.6	×		
				2) 脅迫に対する警報に対応する責任及び手順を明確に定めること	9.5.6	×		
			7) リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末	1) 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること	9.5.7	○		
				2) 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであ	9.5.7	×		
			8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供	1) 既定の時間枠（例えば、バッチファイル伝送のための時間枠）を使うか、又は短時間の通常の対話型処理（session）を用いること	9.5.8	○		
				2) 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること	9.5.8	○		
7.6	業務用ソフトウェアのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	1) 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること	9.6.1	○		
				2) 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮す	9.6.1	○		
				3) 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮	9.6.1	×		
				4) 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること	9.6.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にす	9.6.1	○		
				6) 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること	9.6.1	○		
			2) 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること	1) 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること	9.6.2	×		
				2) 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること	9.6.2	×		
7.7	システムアクセス及びシステム使用状況の監視	認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること	1) 監査記録には、利用者IDを含めること	9.7.1	○		
				2) 監査記録には、ログオン及びログオフの日時を含めること	9.7.1	○		
				3) 監査記録には、可能ならば、端末のID又は所在地を含めること	9.7.1	○		
				4) 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○		
				5) 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○		
			2) 情報処理設備の使用状況を監視する手順を確立すること	1) 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること	9.7.2.1	○		
				2) 監視項目には、認可されているアクセスについて、利用者IDを含むこと	9.7.2.1	○		
				3) 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと	9.7.2.1	○		
				4) 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと	9.7.2.1	○		
				5) 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと	9.7.2.1	○		
				6) 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと	9.7.2.1	○		
				7) 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること	9.7.2.1	○		
				8) 監視項目には、すべての特権操作について、システムの起動及び停止を含めること	9.7.2.1	○		
				9) 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること	9.7.2.1	○		
				10) 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること	9.7.2.1	○		
				11) 監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること	9.7.2.1	○		
				12) 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること	9.7.2.1	×		
				13) 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること	9.7.2.1	○		
				14) 監視項目には、システム警告又は故障について、システム記録例外事項を含めること	9.7.2.1	○		
				15) 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること	9.7.2.1	○		
			3) 監視の結果は、定期的に見直すこと	1) 監視結果の見直しの頻度は、関係するリスクによって決めること	9.7.2.2	×		
				2) 考慮すべきリスク要因には、業務手続に与える重要性の度合を含める	9.7.2.2	×		
				3) 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること	9.7.2.2	×		
				4) 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること	9.7.2.2	×		
				5) 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること	9.7.2.2	×		
			4) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること	1) セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製するこ	9.7.2.3	○		
				2) ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮す	9.7.2.3	○		
				3) 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮	9.7.2.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 記録機能のセキュリティに対して注意すること	9.7.2.3	○		
				5) 管理策は、認可されていない変更及び運用上の問題から保護することを目標とすること	9.7.2.3	○		
			5) コンピュータの時計は正しく設定すること	1) コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時[例えば、万国標準時に（UCT）又は現地の標準時]に合わせること	9.7.3	○		
				2) コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること	9.7.3	○		
7.8	移動型計算処理及び遠隔作業	移動型計算処理及び遠隔作業の設備を用いるときの情報セキュリティを確実にするため	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特	1) 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること	9.8.1	○	ノートPCを利用して、専門家が自宅からリモート接続をおこなう場合、セキュリティ上の保護が不足している可能性を考慮した上での利用に関する個別方針を採用すること。	以前の会議で移動型計算機をありにして、遠隔をなしにするということに決定した。つまり、広口さんが書いているように、緊急時に専門家が自宅からノートPCでリモート接続することを想定する。
				2) 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること	9.8.1	○	ノートPCを利用して、専門家が自宅からリモート接続をおこなう場合の個別方針については、物理的保護、アクセス制御、暗号技術、バックアップ及び、ウィルス対策についての要求事項などを含めること	
				3) 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること	9.8.1	○	ノートPCを利用して、専門家が自宅からリモート接続をおこなう場合の個別方針については、ネットワークに接続する場合の規則及び助言も含めること	ノートＰＣを利用しての接続は、自宅からのみと仮定したが、それでよいか？
				4) 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと	9.8.1	○	ノートPCを利用して、専門家が自宅からリモート接続をおこなう場合は注意をはらうこと	
				5) 悪意のあるソフトウェアに対抗する手順を整えること	9.8.1	○	←	
				6) 悪意のあるソフトウェアに対抗する手順は最新のものであること	9.8.1	○	←	
				7) 移動型計算処理を用いる要員に対する訓練を計画すること	9.8.1	○	ノートPCを利用して、自宅からリモート接続をおこなう専門家に対してセキュリティ教育を実施すること	
							個人情報を含む特に重要な情報については、自宅からのアクセスを禁止もしくは制限すること	この項目は、参考にした「電子政府情報セキュリティ管理基準モデル（庁内ネットワーク）」に含まれていたので追加した。
				8) 情報を素早く、容易にバックアップできる装置が利用可能となっていること	9.8.1	○	○となっているが、N／Aと思います。	
				9) これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること	9.8.1	○	○となっているが、N／Aと思います。	
				10) 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと	9.8.1	○	ノートＰＣに含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと	
				11) ネットワークに接続された移動型設備の使用に対して適切な保護がなされること	9.8.1	○	ネットワークに接続されたノートＰＣの使用に対して適切な保護がなされること	
				12) 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること	9.8.1	○	ノートＰＣを用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること	
				13) 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること	9.8.1	○	ノートＰＣは、盗難に対して物理的に保護されること（可能ならばワイヤーなどで机などに繋ぎ、施錠する）	５．２　５）－２）、３）に移動中のことが書かれているので、ことでは、自宅についてのみ言及すべき？
				14) 大切な、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないこと（可能ならば、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いること）	9.8.1	○	同上	
			2) 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手	1) 遠隔作業の場所に適切な保護が整っていること	9.8.2	×		
				2) 遠隔作業は、経営陣によって認可され、管理されること	9.8.2	×		
				3) 遠隔作業は、この作業形態のため適切に手配されていること	9.8.2	×		
				4) 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること	9.8.2	×		
				5) 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可	9.8.2	×		
				6) 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮	9.8.2	×		
				7) 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮すること	9.8.2	×		
				8) 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること	9.8.2	×		
				9) 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること	9.8.2	×		
				10) 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報の取扱いに慎重を要する度合を考慮	9.8.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				11) 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮	9.8.2	×		
				12) 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの情報又は資源への認可されていないアクセスの脅威を考慮する	9.8.2	×		
				13) 遠隔作業活動のための適切な装置を準備すること	9.8.2	×		
				14) 遠隔作業活動のための適切な保管棚・庫の準備をすること	9.8.2	×		
				15) 遠隔作業活動のための許可される作業を明確にすること	9.8.2	×		
				16) 遠隔作業活動のための作業時間を明確にすること	9.8.2	×		
				17) 遠隔作業活動のための保持してもよい情報の分類を明確にすること	9.8.2	×		
				18) 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること	9.8.2	×		
				19) 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること	9.8.2	×		
				20) 遠隔作業を行う場所の物理的なセキュリティを確保すること	9.8.2	×		
				21) 家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引を明確にすること	9.8.2	×		
				22) ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること	9.8.2	×		
				23) バックアップ及び事業継続のための手順を明確にすること	9.8.2	×		
				24) 監査及びセキュリティの監視を行う	9.8.2	×		
				25) 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること	9.8.2	×		
8.1	システムのセキュリティ要求事項	情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には，管理策についての要求事項を明確にするこ	1) セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること	10.1.1	×		
				2) セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				3) 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考	10.1.1	×		
				4) 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				5) 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること	10.1.1	×		
				6) セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること	10.1.1	×		
				7) セキュリティが確保できなかった場合又はセキュリティが確保されていない場合に起こると思われる業務上の損害の可能性もセキュリティ要求事項及び管理策に反映されこ	10.1.1	×		
8.2	業務用システムのセキュリティ	業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること	1) 業務取引処理(transaction)、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること	10.2.1	×		
				2) 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				3) データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				4) 入力漏れデータ又は不完全なデータを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				5) データ量の上限及び下限からの超過を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				6) 認可されていない又は一貫しない制御データを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				7) 入力データの妥当性及び完全性を確認するために重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること	10.2.1	×		
				8) 入力データに認可されていない変更があるかどうかについての紙に印刷した入力文書の点検を考慮す	10.2.1	×		
				9) 妥当性確認の誤りに対応する手順について考慮すること	10.2.1	×		
				10) 入力データのもっともらしさを試験する手順について考慮すること	10.2.1	×		
				11) データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること	10.2.1	×		
			2) 処理したデータの改変を検出するために，システムに妥当性の検査を組み込むこと	1) 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること	10.2.2.1	×		
				2) データ変更を行う追加・削除の機能を持つプログラムの使用及びその位置について考慮すること	10.2.2.1	×		

業務システムのセキュリティに関しては「監視サービス」は保留とする

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること	10.2.2.1	×		
				4) データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮	10.2.2.1	×		
				5) 取引処理の更新後のデータファイルのバランスをとるための処理又はバッチの制御を考慮すること	10.2.2.1	×		
				6) 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること	10.2.2.1	×		
				7) システム生成データの妥当性確認を考慮すること	10.2.2.1	×		
				8) 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること	10.2.2.1	×		
				9) レコード及びファイルの全体のハッシュ合計の検査を考慮すること	10.2.2.1	×		
				10) 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること	10.2.2.1	×		
				11) プログラムが正しい順序で実行されることの検査を考慮すること	10.2.2.1	×		
				12) プログラムが正しい順序で実行されない場合は終了され、問題が解決するまでは処理が停止することを確実に実施しているかの検査を考慮	10.2.2.1	×		
			3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮す	1) メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと	10.2.3	×		
			4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をするこ	1) 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと	10.2.4	×		
				2) 出力データの妥当性確認には、すべてのデータの処理を確実にするための調整制御の回数を含むこと	10.2.4	×		
				3) 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、読取り装置又はその後の処理システムにとっての十分な情報の供給を含むこと	10.2.4	×		
				4) 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと	10.2.4	×		
				5) 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと	10.2.4	×		
8.3	暗号による管理策	情報の機密性、真正性又は完全性を保護するため	1) 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること	1) 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること	10.3.1	×		
				2) 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を含めた取組みを、考慮すること	10.3.1	○	←	監視サービスにおける暗号は、自宅からつなぐ場合に、VPN,WEBのSSL,SSH対応のtelnetなどが考えられと思います。
			ホスティングに用いるM／Wが暗号化を考慮されている場合△か	3) 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを、	10.3.1	○	←	
			接続サービスのVPNが対象となるか？なる場合△	4) 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について、考慮すること	10.3.1	○	←	
				5) 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について、考慮すること	10.3.1	○	←	
				6) 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを、考慮すること	10.3.1	○	←	
				7) 暗号による管理策の使用に関する個別方針を定めるとき、組織全体にわたって効果的に実施するために採用すべき標準類を考慮すること	10.3.1	○	←	
			2) 取扱いに慎重を要する又は重要な情報の機密性を保護するために，暗号化（Encryption）すること	1) リスクアセスメントに基づき、要求される保護レベルを、使用される暗号アルゴリズムの形式及び品質、並びに使用すべき暗号かぎの長さを考慮して明確にすること	10.3.2	○	←	
				2) 組織における暗号利用の個別方針を実施するとき、世界の異なる地域における暗号技術の使用、及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること	10.3.2	○	←	
				3) 暗号技術の輸出入に適用される規制も考慮すること	10.3.2	○	←	
				4) 適切な保護レベルを明らかにするため、及び要求される保護レベルを提供し、かぎ管理機能をもつ安全な製品を選択するために、専門家の助言を求めること	10.3.2	○	←	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				5) 組織が意図した暗号使用に適用される法令及び規制に関して、必要に応じて法律家の助言を求めること	10.3.2	○	←	
			3) 電子文書の真正性及び完全性を保護するために，ディジタル署名を用いること	1) 秘密かぎの機密性を保護するために注意を払うこと	10.3.3	○		電子文書は監視サービスと関係ないと思います。 ○となっているがN／Aと思います。
				2) 秘密かぎにアクセスした者は、文書に署名でき、その結果かぎの所有者の署名を盗用することがあり得るため、このかぎを秘密に保管するこ	10.3.3	○		○となっているがN／Aと思います。
				3) 公開かぎの完全性を保護すること	10.3.3	○		○となっているがN／Aと思います。
				4) ディジタル署名に使用される暗号かぎは、暗号化に使用されるものとは異なること	10.3.3	○		○となっているがN／Aと思います。
			電子文書の定義 ・業務文書 ・ログを含む監査証跡等 として△とした。	5) ディジタル署名を用いるときは、ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること	10.3.3	○		○となっているがN／Aと思います。
				6) 電子商取引の場合、ディジタル署名の法的位置付けを知ること	10.3.3	○		○となっているがN／Aと思います。
				7) 法的枠組みが不十分である場合、ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること	10.3.3	○		○となっているがN／Aと思います。
				8) 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては、法律家による助言を求める	10.3.3	○		○となっているがN／Aと思います。
			4) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には，否認防止サービスを用いる	（なし）	10.3.4	×		
			5) 一連の合意された標準類，手順及び方法に基づくかぎ管理システムを，暗号技術の利用を支援するために用いること	1) 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること	10.3.5.1	○	←	
				2) すべてのかぎは、変更及び破壊から保護し、共通かぎ及び秘密かぎは、認可されていない露呈から保護	10.3.5.1	○	←	
				3) かぎを生成し、保存し、記録保管するために用いられる装置を保護するためには、物理的保護策を用いること	10.3.5.1	○	←	クライアント側の電子証明書は必要でしょうか？必要がなければ、鍵管理は必要ないのでは？
				4) かぎ管理システムでは、種々の暗号システム及び種々の業務用ソフトウェアのためのかぎを生成する方法を定めること	10.3.5.1	○	←	
			鍵の必要な暗号 ・データ保存 ・通信暗号（共通鍵） ・ログ保存 とした	5) かぎ管理システムでは、公開かぎ証明書を生成し入手する方法を定めること	10.3.5.1	○	←	
				6) かぎ管理システムでは、予定している利用者にかぎを配付する方法を定めること	10.3.5.2	○	←	
				7) かぎ管理システムでは、かぎを保存する方法を定めること	10.3.5.2	○	←	
				8) かぎ管理システムでは、かぎを変更又は更新する方法を定めること	10.3.5.2	○	←	
				9) かぎ管理システムでは、セキュリティが損なわれたかぎを処理する方法について定めること	10.3.5.2	○	←	
				10) かぎ管理システムでは、かぎを無効にする方法について定めること	10.3.5.2	○	←	
				11) かぎ管理システムでは、事業継続管理の一部として、例えば、暗号化された情報の回復のために、消失したかぎ又は損傷したかぎを回復する方法を定めること	10.3.5.2	○	←	
				12) かぎ管理システムでは、かぎを、例えば、記録保管された情報又はバックアップされた情報などのために、記録保管する方法について定める	10.3.5.2	○	←	
				13) かぎ管理システムでは、かぎを破壊する方法を定めること	10.3.5.2	○	←	
				14) かぎ管理システムでは、かぎ管理に関連する活動を記録し監査する方法を定めること	10.3.5.2	○	←	
				15) かぎ管理システムでは、セキュリティが損なわれる可能性を軽減するために、かぎは一定期間だけ用いることができるように、かぎの活性化及び非活性化の期日を定めるこ	10.3.5.2	○	←	
				16) かぎの活性化及び非活性化の期間は、暗号による管理策が使用される環境及び認識されているリスクによって決めること	10.3.5.2	○	←	
				17) 安全に管理された共通かぎ及び秘密かぎの問題に加え、公開かぎの保護についても考慮すること	10.3.5.2	○	←	
				18) 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に	10.3.5.2	○	←	
8.4	システムファイルのセキュリティ	ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にする	1) 運用システムでのソフトウェアの実行を管理すること	1) 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること	10.4.1	○		
				2) 運用システムは、実行可能なコードだけを保持すること	10.4.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れの確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しな	10.4.1	○		
				4) 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること	10.4.1	○		
				5) 古い版のソフトウェアは、事故対策用として保持すること	10.4.1	○		
				6) 運用システムに使用されるベンダー供給ソフトウェアは、供給者によって支援されるレベルで、維持管理され	10.4.1	○		
				7) 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること	10.4.1	○		
				8) セキュリティ上の欠陥を除去するか又は軽減するのに役立つ場合には、ソフトウェアパッチを適用するこ	10.4.1	○		
				9) 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること	10.4.1	○		
				10) 供給者の活動は監視されることが望ましい	10.4.1	○		
			2) 試験データを保護し，管理すること	1) システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと	10.4.2	○		
				2) 個人情報が入っている運用データベースは、使用しないようにすること	10.4.2	○		
				3) 個人情報が入っている情報を使用する場合は，使用する前に，個人的要素を消去すること	10.4.2	○		
				4) 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用	10.4.2	○		
				5) 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けるこ	10.4.2	○		
				6) 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること	10.4.2	○		
				7) 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること	10.4.2	○		
			3) プログラムソースライブラリへのアクセスに対しては，厳しい管理を維持す	1) 可能な限り、プログラムソースライブラリは、運用システムに含めないこと	10.4.3	×		
				2) 各アプリケーションごとに、プログラムライブラリ管理責任者を任命する	10.4.3	×		
				3) IT支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと	10.4.3	×		
				4) 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと	10.4.3	×		
				5) その業務用ソフトウェアのためのIT支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プログラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること	10.4.3	×		
				6) プログラムリストは、セキュリティの保たれた環境に保持されること	10.4.3	×		
				7) プログラムソースライブラリへのすべてのアクセスについて、監査記録を維持管理すること	10.4.3	×		
				8) ソースプログラムの旧版は、記録保管しておくこと	10.4.3	×		
				9) 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと	10.4.3	×		
				10) プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従うこと	10.4.3	×		
8.5	開発及び支援過程におけるセキュリティ	業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理すること	1) 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないこと	10.5.1	○		
				2) 支援プログラマによるシステムへのアクセスはその作業に必要な部分に限定されること	10.5.1	○		
				3) 変更に対する正式な合意及び承認が得られていることを確実にするこ	10.5.1	○		
				4) 業務用ソフトウェア及び運用の変更管理手順は統合されること	10.5.1	○		
				5) 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること	10.5.1	○		
				6) 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確実にすること	10.5.1	○		
				7) 業務用ソフトウェア及び運用の変更過程では、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするためにこの手順をレビューすること	10.5.1	○		
				8) 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識	10.5.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				9) 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を	10.5.1	○		
				10) 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること	10.5.1	○		
				11) 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること	10.5.1	○		
				12) 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新されること	10.5.1	○		
				13) 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実に	10.5.1	○		
				14) 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェアの更新について版数の管理を行うこと	10.5.1	○		
				15) 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること	10.5.1	○		
				16) 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること	10.5.1	○		
				17) 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること	10.5.1	○		
			2) オペレーティングシステムを変更した場合は，業務用システムをレビューし，試験すること	1) オペレーティングシステムの変更によって業務用ソフトウェアの管理及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること	10.5.2	○		
				2) 年間支援計画及び予算には、オペレーティングシステムの変更の結果として必要となるレビュー及びシステム試験を必ず含めるようにするこ	10.5.2	○		
				3) 実施前に行う適切なレビューに間に合うように、オペレーティングシステムの変更を通知することを確実にす	10.5.2	○		
				4) 事業継続計画に対して適切な変更がなされることを確実にすること	10.5.2	○		
			3) パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更を厳しく管理すること	1) ベンダー供給のパッケージソフトウェアは、変更しないで使用すること	10.5.3	○		
				2) パッケージソフトウェアの変更が絶対必要であると判断された場合は、組み込まれている管理策及び完全性の処理が損なわれるリスクを考	10.5.3	○		
				3) パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること	10.5.3	○		
				4) パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる可能性を考慮すること	10.5.3	○		
				5) パッケージソフトウェアの変更が絶対必要であると判断された場合は、変更の結果として、将来のソフトウェア保守に対して組織が責任を負うようになるかどうかの影響を考慮	10.5.3	○		
				6) 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと	10.5.3	○		
				7) 変更はすべて、完全に試験すること	10.5.3	○		
				8) 変更はすべて、文書化すること	10.5.3	○		
				9) 将来更新されたソフトウェアに再び適用できるようにすること	10.5.3	○		
			4) 隠れチャネル（Covert channels）及びトロイの木馬（Trojan code）の危険性から保護するために，ソフトウェアの購入，使用及び修正を管理し，検査すること	1) プログラムは定評のある開発元のものだけを購入すること	10.5.4	○		
				2) コードの確認ができるようにソースコードでプログラムを購入すること	10.5.4	○		
				3) 評価された製品を用いること	10.5.4	○		
				4) 使用前にすべてのソースコードを検査すること	10.5.4	○		
				5) 一旦導入したコードへのアクセス及びそのコードへの変更を管理するこ	10.5.4	○		
				6) 重要なシステムでの作業には確実に信頼できる要員を用いること	10.5.4	○		
			5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために，管理策を用いるこ	1) ソフトウェア開発を外部委託する場合、使用許諾に関する取決め、コードの所有権及び知的所有権について考慮すること	10.5.5	×		
				2) ソフトウェア開発を外部委託する場合、実施される作業の質及び正確さの認証を考慮すること	10.5.5	×		
				3) ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託（escrow）契約に関する取決めについて考慮すること	10.5.5	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) ソフトウェア開発を外部委託する場合、なされた作業の質及び正確さの監査のためのアクセス権について考慮すること	10.5.5	×		
				5) ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること	10.5.5	×		
				6) ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること	10.5.5	×		
9.1	事業継続管理の種々の面	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため	1) 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること	1) 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること	11.1.1	×		
				2) 業務手続の中断が事業に及ぼすと思われる影響を理解し（組織の存続性を脅かす可能性のある重大な事件・事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である）、情報処理施設の事業目的を確立すること	11.1.1	×		
				3) 事業継続の手続の一部をなすこともある適切な保険への加入を考慮	11.1.1	×		
				4) 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること	11.1.1	×		
				5) 合意された戦略に従って事業継続計画を明確にし、文書化すること	11.1.1	×		
				6) 実行されている計画及び手続を定期的に試験し、更新すること	11.1.1	×		
				7) 事業継続管理が組織の手続及び機構に確実に組み込まれるようにする	11.1.1	×		
				8) 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること	11.1.1	×		
			2) 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めるこ	1) それらの障害の影響（損害規模及び回復期間の両面から）を判断するために、リスクアセスメントを行うこと	11.1.2	×		
				2) これら両活動の実施には、事業資源及び手続の管理者が全面的に関与すること	11.1.2	×		
			3) 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てるこ	1) 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること	11.1.2	×		
			4) 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること	1) 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること	11.1.3	×		
				2) 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施す	11.1.3	×		
				3) 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に注意すること	11.1.3	×		
				4) 事業継続計画の作成過程では、合意された手順及び過程を文書化す	11.1.3	×		
				5) 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと	11.1.3	×		
				6) 事業継続計画の作成過程では、計画の試験及び更新を行うこと	11.1.3	×		
				7) 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと	11.1.3	×		
				8) これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること	11.1.3	×		
			5) すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること	1) 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること	11.1.4	×		
				2) 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正す	11.1.4	×		
				3) 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件を考慮すること	11.1.4	×		
				4) 事業継続計画作成の枠組みでは、事業運営及び/又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること	11.1.4	×		
				5) 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決めを含むこと	11.1.4	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の手順について考慮すること	11.1.4	×		
				7) 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること	11.1.4	×		
				8) 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表について考慮すること	11.1.4	×		
				9) 事業継続計画作成の枠組みでは、事業継続手続を理解させ、手続が継続して有効であることを確保するために計画される認識及び教育活動について考慮すること	11.1.4	×		
				10) 事業継続計画作成の枠組みでは、個人の責任について考慮すること	11.1.4	×		
				11) 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するのに誰が責任をもつかを記述すること	11.1.4	×		
				12) 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること	11.1.4	×		
				13) 事業継続計画作成の枠組みでは、各計画には特定の責任者がいるこ	11.1.4	×		
				14) 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること	11.1.4	×		
				15) 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者の責任とすること	11.1.4	×		
			6) 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること	1) 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職員がそれらの計画を確実に認識するものであること	11.1.5.1	×		
				2) 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと	11.1.5.1	×		
				3) 計画の個々の構成要素を、頻繁に試験すること	11.1.5.1	×		
				4) 計画が実際に役立つことを保証するために、様々な手法を使用するこ	11.1.5.1	×		
				5) 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画の検討）	11.1.5.1	×		
				6) 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）	11.1.5.1	×		
				7) 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）	11.1.5.1	×		
				8) 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施す	11.1.5.1	×		
				9) 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）	11.1.5.1	×		
				10) 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験す	11.1.5.1	×		
				11) いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反映させること	11.1.5.1	×		
			7) 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること	1) 事業継続上の問題を適切に対処することを確実にするための手順は、組織の変更管理プログラムの中に含まれること	11.1.5.2	×		
				2) 各事業継続計画の定期的見直しに対する責任を割り当てること	11.1.5.2	×		
				3) 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に更新すること	11.1.5.2	×		
				4) この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること	11.1.5.2	×		
10.1	法的要求事項への適合	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避ける	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項に適合する特定の管理策、及び個々の責任も同様に明確に定め、文書化すること	12.1.1	×		
			2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は，法的制限事項に適合するように，適切な手続を実行す	1) ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること	12.1.2.2	×		
				2) ソフトウェア製品の取得手続に関する標準類を発行すること	12.1.2.2	×		
				3) ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること	12.1.2.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 適切な財産登録簿を維持管理すること	12.1.2.2	×		
				5) 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること	12.1.2.2	×		
				6) 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること	12.1.2.2	○		
				7) 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確認すること	12.1.2.2	○		
				8) 適切な使用許諾条件を維持管理するための個別方針を定めること	12.1.2.2	×		
				9) ソフトウェアの処分又は他人への譲渡についての個別方針を定めること	12.1.2.2	×		
				10) 適切な監査ツールを用いること	12.1.2.2	×		
				11) 公衆ネットワークから入手するソフトウェア及び情報の使用条件に従うこ	12.1.2.2	×		
			3) 組織の重要な記録は、消失、破壊及び改ざんから保護されること	1) 記録類は、記録の種類（例えば、会計記録、データベース記録、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について保持期間及び記録媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光学媒体）の詳細も定めておく	12.1.3	×		
				2) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること	12.1.3	○		
				3) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、必要なときに、認可されている者が使用できるようにすること	12.1.3	○		
				4) 記録の保管に用いられる媒体が劣化する可能性を考慮すること	12.1.3	×		
				5) 保管及び取扱いの手順は、製造業者の推奨に従って実行すること	12.1.3	×		
				6) 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確保する手順を	12.1.3	×		
				7) 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式で取り出すことができるように、データ保管システムを選択すること	12.1.3	×		
				8) 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にす	12.1.3	×		
				9) 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること	12.1.3	×		
				10) 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行す	12.1.3	×		
				11) 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること	12.1.3	×		
				12) 主要な情報の出典一覧を維持管理すること	12.1.3	×		
				13) 重要な記録及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実行すること	12.1.3	○ 監視ﾛｸﾞ		
			4) 関連する法令に従って個人情報を保護するために，管理策を用いること	1) データ保護の担当責任者を任命すること	12.1.4	×		
				2) 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当責任者に報告することは、データ所有者の責任であること	12.1.4	×		
				3) 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任で	12.1.4	×		
			5) 情報処理施設の使用には管理者の認可を要するものとし，そのような施設の誤用を防ぐための管理策を用いること	1) 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされること	12.1.5	×		
				2) 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること	12.1.5	×		
				3) 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること	12.1.5	×		
				4) すべての利用者は、その許可されたアクセスの正確な範囲を認識していること	12.1.5	×		
				5) 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを通知すること	12.1.5	×		
				6) ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告ﾒｯｾｰｼﾞをコンピュータの画面上に表	12.1.5	○		
				7) 利用者は、引き続きログオン処理を行うために画面上のﾒｯｾｰｼﾞに同意し、それに適切に対応すること	12.1.5	×		
			6) 暗号による管理策の策定においては、国の法律への適合を確実なものにするために，法的な助言を求めること	1) 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること	12.1.6	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	監視サービス		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
			7) 人又は組織に対する措置を支援するには，十分な証拠をもつこと	1) 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること	12.1.7.1	×		
				2) 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとる	12.1.7.1	×		
				3) 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること	12.1.7.3	×		
				4) コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっ	12.1.7.3	○		
				5) コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること	12.1.7.3	×		
				6) コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること	12.1.7.3	×		
				7) 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得る	12.1.7.3	×		
10.2	セキュリティ基本方針及び技術適合のレビュー	組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため	1) 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること	1) 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること	12.2.1	×		
				2) 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること	12.2.1	×		
			2) 情報システムは，セキュリティ実行標準と適合していることを定期的に検査すること	1) 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行	12.2.2	○		
				2) 技術適合の検査では、専門家の技術援助を得ること	12.2.2	×		
				3) 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアによって実施されるこ	12.2.2	○		
				4) 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること	12.2.2	×		
				5) いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施さ	12.2.2	×		
10.3	システム監査の考慮事項	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意され	1) 監査要求事項は、担当経営陣の同意を得ること	12.3.1	×		
				2) 検査の範囲は、合意され、管理されること	12.3.1	×		
				3) 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定するこ	12.3.1	×		
				4) 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること	12.3.1	×		
				5) 複製ファイルは、監査が完了した時点で消去すること	12.3.1	×		
				6) 検査を実施するための情報資源は、明確に識別され、利用可能であ	12.3.1	×		
				7) 特別又は追加処理の要求事項は、識別され、合意されること	12.3.1	×		
				8) すべてのアクセスは、照合用の証跡を残すために、監視され、記録さ	12.3.1	×		
				9) すべての手順、要求事項及び責任について、文書化すること	12.3.1	×		
			2) システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること	1) システム監査ツールは、開発及び運用システムから分離しておくこと	12.3.2	×		
				2) システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと	12.3.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
5.1	セキュリティが保たれた領域	業務施設及び業務情報に対する認可されていないアクセス、損傷及び妨害を防止するため	1) 組織は、情報処理設備を含む領域を保護するために、幾つかのセキュリティ境界を利用すること	1) セキュリティ境界を明確に定義すること	7.1.1	○	情報資産の重要度に応じて、フロアー・部屋・中間間仕切り等によるスペース単位で明確にゾーニング（境界）化されていること。	物理的セキュリティについては、以下の観点について、掘り下げる方針とする。
				2) 情報処理設備を収容した建物又は敷地の境界は、物理的に頑丈であること	7.1.1	○	敷地の境界（外周壁など）、建物及び室内の間仕切りは破壊されにくい仕様となっていること。	・構造的なもの（壁の強度等） ・設備環境（空調、電源、消火設備等） ・セキュリティ技術（生態認証等）
				3) 敷地の外周壁を堅固な構造物とすること、及びすべての外部扉を認可されていないアクセスから開閉制御の仕組み（かんぬき、警報装置、錠など）で適切に保護すること	7.1.1	○	外周壁などの門、建物の出入口及び室内の間仕切りにおける開口部には扉が付加され、施錠管理がなされていること。	・監視装置（監視カメラ等）
				4) 敷地又は建物への物理的アクセスを管理するために、有人の受付又はその他の手段を設けること	7.1.1	○	建物の出入口及び室内の間仕切りにおける開口部の人の出入は有人受付または入退管理システムにより管理されていること。	
				5) 敷地及び建物へのアクセスは、認可された職員だけに制限すること	7.1.1	○	建物の出入口及び室内の間仕切りにおける開口部の出入は許可された人に制限されていること。	
				6) 物理的な壁は、床から天井にわたる構造で設けること	7.1.1	○	室内の間仕切りは天井まで人が越えられないように設計されていること。	
				7) セキュリティ境界上にあるすべての防火扉は、警報装置付き及び密閉式であること	7.1.1	○	建物及び室内の間仕切りの扉には防火対策が施され、警報装置も配されていること。	
			2) 認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によってセキュリティの保たれた領域を保	1) セキュリティが保たれた領域への訪問者を監視すること	7.1.2	○	建物の出入口及び室内の間仕切りにおける開口部の出入監視のための監視カメラが設置されていること。	
				2) セキュリティが保たれた領域への訪問者に立ち入り許可を求めさせること	7.1.2	×		
				3) セキュリティが保たれた領域への入退の日付・時間を記録すること	7.1.2	○	建物の出入口及び室内の間仕切りにおける開口部からの入退場時の日付・時間を記録する（ログを取る）しくみになっていること。	
				4) セキュリティが保たれた領域への訪問者には、認可された特定の目的に限ってのアクセスを認めること	7.1.2	○	建物の出入口及び室内の間仕切りにおける開口部から入場する人は、許可された特定の目的に限って立ち入り許可を受けるしくみになっていること。	
				5) セキュリティが保たれた領域への訪問者その領域のセキュリティ要求事項及び非常時の手順を説明した文	7.1.2	×		
				6) 取扱いに慎重を要する情報及び情報処理設備へのアクセスを管理すること	7.1.2	○	情報およびコンピュータへのアクセスの日付・時間を記録する（ログを取る）しくみになっていること。	
				7) 取扱いに慎重を要する情報及び情報処理設備へのアクセスは認可された者だけに制限すること	7.1.2	○	情報処理設備が収納されている部屋への出入は許可された人に制限されていること。	
				8) アクセスをすべて認可して、暗証番号付きの磁気カードといった認証管理策を用いること	7.1.2	○	アクセスを認可する手段として、個人識別認証管理策（暗証番号付き磁気カード、ICカードまたはバイオメトリクス認証等）により入退場した人の識別・記録をとる（ログを取る）しくみになっていること。	
				9) すべてのアクセスの監査証跡は、安全に保管しておくこと	7.1.2	○	建物の出入口及び室内の間仕切りにおける開口部からの入退場時の記録（ログ）は一定期間安全に保管するしくみになっていること。	
				10) すべての要員に、目に見える何らかの形状をした身分証明の着用を要求すること	7.1.2	×		
				11) 付添いを伴わない見知らぬ人及び目に見える身分証明を着用していない人に対しては、誰であるか問い掛けるよう奨励すること	7.1.2	×		
				12) セキュリティが保たれた領域へのアクセス権は、定期的に見直し及び更新すること	7.1.2	○	建物の出入口及び室内の間仕切りにおける開口部の出入が許可された人の制限は、定期的に見直し及び更新されることになっていること。	
			3) セキュリティが保たれた領域の選択及び設計においては、火災、洪水、爆発、騒擾、その他の自然又は人為的災害による損害の可能性を考慮すること	1) 関連する健康及び安全に関する規制並びに標準類も考慮に入れること	7.1.3	×		
				2) 隣接場所から及んでくるセキュリティ上のいかなる脅威についても考慮すること	7.1.3	○	建物は、隣接敷地・施設が影響する漏洩・破壊・改ざん・災害（火災・水害など）等の脅威の可能性を考慮していること。	
				3) 主要な設備は、一般の人のアクセスが避けられる場所に設置すること	7.1.3	○	設備機器は、立ち入りを許可されている人以外がなるべく近づけない配置となるよう考慮されていること。	
				4) 建物は目立たせず、その用途を示	7.1.3	×		
				5) 情報処理作業の存在を示すものは	7.1.3	×		
				6) 複写機、ファクシミリといった支援機能及び装置は、セキュリティの保たれた領域内の適切な場所に設置すること	7.1.3	○	ファクシミリ、複写機、印字装置（プリンター・プロッター等）など守るべき情報資産を排出する装置は、セキュリティの確保された適切な場所に設置されていること。（来訪者に存在がわからないように、間仕切り等で仕切るなど専用スペースとする。）	
				7) 要員が不在のときは扉及び窓に施錠すること	7.1.3	×		
				8) 一階の窓については、外部に対する防御を考慮すること	7.1.3	○	施設(室）へ乗移り（隣接する室の窓からの侵入・屋上からのつたい降り等含む）など外部からの不正なアクセスに対する防護を考慮していること。	
				9) すべての外部扉及びアクセス可能な窓には、適切な侵入者の検知システムを設置すること	7.1.3	○	建物・施設のすべての外部扉及びアクセス可能な窓には、侵入者の検知・通報のしくみを考慮していること。	

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				10) 侵入者の検知システムは、専門の標準類に従って取り付けられること	7.1.3	○	建物・施設（室）に設置した、侵入者の検知・通報のしくみは専門の防犯設備規定に従って取り付けられていること。	
				11) 侵入者の検知システムは、定期的に点検すること	7.1.3	○	建物・施設（室）に設置した、侵入者の検知・通報のしくみは定期的に点検、確認されていること。	
				12) 無人の領域には常に警報装置を稼働させること	7.1.3	○	無人の施設（室）における侵入者の検知・通報のしくみ（警報・通報装置など）は常に稼動状態にあるか。	
				13) コンピュータ室又は通信室といった他の領域においても、警報装置を設置すること	7.1.3	○	コンピュータ室又は通信設備室には、不慮の事故（侵入・破壊・災害等）における検知・通報のしくみを考慮していること。	
				14) 組織自ら管理する情報処理設備は、第三者が管理するものから物理的に分離しておくこと	7.1.3	○	組織自ら保有する情報資産は第三者（部外者など）が管理している情報資産と物理的に（保管場所等）に分離していること。	
				15) 取扱いに慎重を要する情報処理設備の所在を掲げた職員録及び社内電話帳は、一般の人に容易に見られないようにすること	7.1.3	×		
				16) 危険物又は可燃物は、セキュリティが保たれた領域から十分に離れた場所に、安全に保管すること	7.1.3	○	危険物または可燃物は建物・施設（室）等と離して安全に保管するようになっていること。	
				17) セキュリティが保たれた領域には、事務用品などを、必要もないのに大量に保管しないこと	7.1.3	×		
				18) 緊急時に用いる代替装置及びバックアップされた媒体は、主事業所から十分に離れた場所に置くこと	7.1.3	○	守るべき情報資産とそのバックアップ情報資産は,互いに十分離れた場所に保管されていること。	
			4) セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理	1) セキュリティが保たれた領域の存在又はそこでの作業は、その必要がある要員だけが知っていること	7.1.4	○	建物・施設（室）の存在や、そこでの作業内容は、普段業務を行っている場所から十分に離れた場所に置くこと	
				2) セキュリティが保たれた領域において監視もなく作業することは、避けること	7.1.4	○	建物・施設（室）における立入及び作業においては、何らかの監視下にあること。	
				3) セキュリティが保たれた領域を無人にするときは、物理的な施錠を行うこと	7.1.4	○	建物・施設（室）が無人の場合は、施錠されていること。	
				4) セキュリティが保たれた領域を無人にするときは、定期的に検査すること	7.1.4	○	建物・施設（室）が無人の場合は、情報資産に異常がないかを定期的に確認することになっていること。	
				5) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスを許可するときは、アクセスができる範囲を限定し、アクセスが必要な場合に限ること	7.1.4	○	建物・施設（室）または情報資産に対する外部支援サービス関係者の立ち入り許可をする場合の条件としては、外部支援サービスは必要な場合に限り、なおかつ立入範囲を限定するようになっていること。	
				6) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは認可のもとにおくこと	7.1.4	○	建物・施設（室）または情報資産に対して外部支援サービス関係者が立ち入る場合は許可制として管理されていること。	
				7) セキュリティが保たれた領域又は取扱いに慎重を要する情報処理設備に外部の支援サービス要員のアクセスは監視下におくこと	7.1.4	○	建物・施設（室）対して立入及び作業員のアクセスは、何らかの監視下にあること。	
				8) あるセキュリティ境界の中にセキュリティ要求事項の異なる領域が存在するときは、その領域の間に、物理的アクセスを管理するための障壁及び境界を追加すること	7.1.4	○	施設(室）にその情報資産と別の（セキュリティ要求事項の異なる）情報資産が存在するときは、その情報資産単位に間仕切り等の境界が設けられていること。	
				9) 認可なしの、写真機、ビデオカメラ、録音機、又はその他の記録装置の使用は、許さないこと	7.1.4	×	建物・施設（室）においては、許可されていない記録装置、通信装置（写真機・ビデオカメラ・録音機・携帯電話・その他事務用品、備品など）の使用はできないようになっていること。	
			5) 品物を受け渡しする場所について管理し、可能ならば、認可されていないアクセスを回避するために、情報処理設備から隔	1) 品物を受け渡しする場所についてのセキュリティ要求事項は、リスクアセスメントに基づいて決定すること	7.1.5	○	物品の受渡しの場所は、他の施設（室）と境界を設けられており、アクセス制限がかけられていること。	印刷物エリアを含むファシリティとして対象に含める。
				2) 建物の外から一時保管場所へのアクセスは、本人の確認及び認可を受けた要員に限定すること	7.1.5	○	建物・施設（室）の外部から物品集配のために物品受渡しの場所（一時保管場所）へ出入する集配人は事前に身分確認と入室許可を受けた者のみに限定されていること。	
				3) 一時保管場所については、建物内の他の場所にアクセスすることなく受渡しの要員が荷おろしできるように、設計を行うこと	7.1.5	○	建物・施設の外部から物品集配のためにアクセスする集配人が、他の施設（室）へ出入することなく物品受渡しの場所（一時保管場所）で荷おろし・荷受ができるようになっていること。	
				4) 一時保管場所の内部扉を開いているときは、外部扉を締めること	7.1.5	○	建物・施設（室）の外部との物品受渡しの場所（一時保管場所）は、内扉が開いているときは外扉を閉めて、同時開放とならないようになっていること。	
				5) 一時保管場所から使用場所に搬入品を移送する前に、危険の可能性がないかどうか、その品物を検査すること	7.1.5	○	建物・施設（室）の外部から物品受渡しの場所（一時保管場所）で荷受された物品を使用場所に移す前に、物品の危険性を検査するようになっていること。	
				6) 敷地内に搬入するときには、搬入品の登録を行うこと	7.1.5	○	建物・施設（室）の外部から直接施設内（敷地含む）のいずれかに物品が搬入される場合においては、その搬入品の登録をいずれかの場所で行うようになっていること。	
5.2	装置のセキュリティ	資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため	1) 装置は、環境上の脅威及び危険からのリスク並びに認可されていないアクセスの可能性を軽減す	1) 装置は、作業領域への不必要なアクセスが最小限に抑えられる位置に設置すること	7.2.1	○	装置の重要度に応じてゾーニングを行い、各ゾーンごとにガードマンの設置による監視や、アクセス制御（施錠、カード、生体認証等のシステム）を設け、作業領域への不必要なアクセスを最小限にすること。	ここでは、各サービスにおける次の装置等を想定する。
				2) 取扱いに慎重を要するデータを扱う情報処理設備及び記憶装置は、使用中に盗み見されるリスクを軽減するように設置すること	7.2.1	○	端末は、使用中に盗み見されるリスクを軽減するため、操作者の肩越しから覗き見ができないように設置すること。また、フィルタを設置し、視認できる範囲を限定すること。	・マシンレンタルサービス：レンタル用サーバおよび通信機器。

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				3) 特別な保護を必要とする装置は、要求される一般の保護水準より下げないために、分離して設置すること	7.2.1	○	厳重な保護を必要とする装置の保護水準を下げないために、装置の重要度に応じてゾーニングを行い、アクセス制御を設け、一般の保護水準装置とは分離して設置するこ	・接続サービス：インターネット接続に必要な、FWサーバおよびルータ等の通
				4) 組織は、情報処理設備の周辺での飲食及び喫煙についての個別方針の策定を考慮すること	7.2.1	×		・監視サービス：監視用の端末等
				5) 周辺の環境状態が、情報処理設備の運用に悪影響を及ぼすかどうか、その状況を監視すること	7.2.1	○	居室及びサーバ室の周辺に関して、ネットワーク対応環境監視装置等センサーを設置し、監視すること。	・ファシリティ：入退館管理装置、監視カメラ等
				6) 作業場などの環境で使用する装置には、キーボードカバーのような特別な保護具の使用を考慮すること	7.2.1	○	端末は、誤動作ができるだけ行われないよう、また、塵埃等の影響から保護するために、キーボードカバー等を使用すること。	
				7) 近隣の敷地に起こる災害（例えば、建物の火災、屋根からの水漏れ、地下室の浸水、又は道路での爆発）の影響を考慮すること	7.2.1	×		
			2) 装置は、停電、その他の電源異常から保護すること	1) 装置は、装置製造者の仕様に適合した適切な電力の供給を確保すること	7.2.2	○	各装置製造者から提出されている各装置の緒元合計値をベースにし、必要な電力を算出すること。システム維持の需要容量とは別に、突入電力や将来の増設電力、負	
				2) 電源の多重化をすること	7.2.2	○	主電源が故障した場合に備え、別の電源を用意しておく	
				3) 無停電電源装置（UPS）を設置する	7.2.2	○	装置に必要な品質の電力を供給するため、UPSを設置	
				4) 非常用発電機の設置をすること	7.2.2	○	装置の安定稼動を図るため、非常用発電機を設置するこ	
				5) 障害対策計画では、UPSが故障した場合に取るべき措置についても計画しておくこと	7.2.2	○	障害対策計画においては、UPSが故障した場合に備え、UPSと非常用発電機との組合せ、UPSと2系統受電の組合せ等を計画しておくこと。	
				6) UPSは、容量が十分であることを定期的に確認すること	7.2.2	○	UPSの供給余裕度が需要要領に対して20%以上となるよう定期的に確認すること。	
				7) UPSは、製造者の推奨に従って点検すること	7.2.2	○	障害発生時の2次電源として確実に非常時に使用できるようUPSは製造者の推奨に従って点検すること。	
				8) 長時間にわたる停電の場合でも処理を継続しなければならない場合には、非常用発電機を考慮すること	7.2.2	○	長時間にわたる停電においても、情報処理業務を継続する必要がある場合には、非常用発電機を設置し、予備機常時並列方式または予備機スタンバイ方式を採用すること	
				9) 発電機を使用する場合、製造者の推奨に従って定期的に点検すること	7.2.2	○	障害発生時の2次電源として確実に非常時に使用できるよう発電機は製造者の推奨に従って点検すること。	
				10) 発電機を長時間運転できるように、燃料の十分な供給を確保すること	7.2.2	○	非常用発電機が長時間運転できるよう軽重油及び液化石油ガス等燃料の十分な供給を確保すること。	
				11) 電源の緊急スイッチは、機械室の非常口近くに設置すること	7.2.2	○	緊急時、人を安全に非難、誘導するため、電源のスイッチは機械室の非常口近くに設置すること。	
				12) 主電源の停電時用として非常用照明を備えること	7.2.2	○	主電源の停電時においても、人が避難、誘導を迅速に行えるよう各室および廊下、階段等通路に非常照明設備又	
				13) 落雷防護はすべての建物に備えること	7.2.2	○	雷害による被害から防護するため、避電設備を設置すること	
				14) すべての外部通信回線に落雷防護フィルタを付けること	7.2.2	○	雷サージによる異常電圧から装置を防護するため、外部通信回線には落雷防護フィルタを取り付け、信号用避雷	
			3) データ伝送又は情報サービスに使用する電源ケーブル及び通信ケーブルの配線は、傍受	1) 情報処理設備に接続する電源ケーブル及び通信回線は、可能ならば地下に埋設するか、又はそれに代わる十分な保護手段を施すこと	7.2.3	○	電源ケーブル及び通信ケーブルは、電磁界の影響や傍受から保護するため、可能であれば地中ケーブルとすること。また、通信ケーブルは可能であれば光ファイバーケーブルとすること。	
				2) ネットワークのケーブル配線を、認可されていない傍受又は損傷から保護すること	7.2.3	○	通信ケーブルは、容易に接触することで損傷したり、傍受できないよう、床下や天井裏への配線を用い、専用管とすること。	ネットワークケーブルに関する管理は、各サービスに付随するハードウェアの一
				3) 干渉を防止するために、電源ケーブルは通信ケーブルから隔離すること	7.2.3	○	電源ケーブルと通信ケーブルは、電磁妨害（EMI）や電波干渉（RFI）といった干渉を防止するため、管路を分離す	
				4) 取扱いに慎重を要するシステム又は重要なシステムに対しては、外装電線管の導入をすること	7.2.3	○	重要な機能を有する装置は、外装電線管を導入すること。	
				5) 取扱いに慎重を要するシステム又は重要なシステムに対しては、点検箇所・終端箇所を施錠可能な部屋又はボックス内に設置すること	7.2.3	○	重要なシステムに接続されているネットワークの点検箇所、終端箇所については、施錠可能な部屋、ラック、ボックス内に設置すること。	
				6) 取扱いに慎重を要するシステム又は重要なシステムに対しては、代替経路又は伝送媒体を使用すること	7.2.3	○	システムが中断された場合の影響度に応じてネットワーク配線を二重化し、常用待機、負荷分散などの冗長構成を採ること。	
				7) 取扱に慎重を要するシステム又は重要なシステムに対しては、光ファイバケーブルを使用すること	7.2.3	○	傍受や干渉が起こった場合の影響度に応じて、光ファイバーケーブルを使用すること。	
				8) 認可されていない装置がケーブルに取り付けられていることどうかについての調査すること	7.2.3	○	スイッチングハブ等で使用していない接続ポートは無効設定とするか、封印し、許可無く使用されていないか定期的に確認すること。検疫ネットワークシステムを導入し、監視	
			4) 装置についての継続的な可用性及び完全性の維持を確実とするために、装置の保守を正しく	1) 装置は、供給者の推奨する整備間隔及び仕様書に従って、保守を実施すること	7.2.4	○	供給者の推奨整備間隔及び仕様書等であらかじめ定められた整備間隔に基づき、装置の保守作業を実施すること。	
				2) 認可された保守担当者だけが装置の修理及び手入れを実施すること	7.2.4	○	装置の修理及び手入れは、保守契約先からの担当者、あるいはあらかじめ定められた者のみが実施すること。作	
				3) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守について記録すること	7.2.4	○	装置について、何らかの障害が発生した場合には、その大小に係わらず、その障害内容を記録すること。また、障害の予防及び是正するために実施した保守について、その保守内容を記録すること。	
				4) すべての実際に起こっている障害又は障害と考えられるもの、並びにすべての予防及び是正のための保守についての記録を保管すること	7.2.4	○	装置の障害記録及び障害の予防及び是正のための保守内容記録は、保守対象の装置とは別の媒体で保管すること。	
				5) 装置を保守するために搬出する場合、適切な管理策を施すこと	7.2.4	○	装置を保守するために搬出する場合、データをバックアップした後、消磁装置を用いて完全消去し、データがアクセ	
				6) 保険約款によって定められたすべての要求事項に従うこと	7.2.4	×		
			5) 所有権に関係なく、組織の敷地外で情報処理のために装置を使用する場合は、管理者が認可	1) 実施するセキュリティは、組織の敷地外における作業のリスクを考慮に入れること	7.2.5	×		接続サービス、監視サービスにおいて、専門家が自宅よりリモート接続して操作することを想定している。
				2) 事業所外にもち出した装置及び媒体は一般の場所に放置しないこと	7.2.5	×		
				3) ポータブルコンピュータは、外出時には、手荷物としてもち運び、可能ならば見せないようにすること	7.2.5	×		
				4) 装置の保護に関しては、製造者の指示に常に従うこと	7.2.5	×		
				5) 在宅作業についての管理策は、リスクアセスメントによって決定すること	7.2.5	×		
				6) 在宅作業について、適切な管理策（施錠可能な文書保管庫、クリアデスク方針及びコンピュータのアクセス制御等）を適用すること	7.2.5	×		
				7) 事業所外の装置を保護するために、十分な保険が付保されていること	7.2.5	×		
				8) セキュリティリスクを考慮し、それぞれの場所に応じた最も適切な管理策を導入すること	7.2.5	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			6) 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するか又は、確実に	1) 固定ハードディスクといった記憶媒体を内蔵している装置は、すべて処分する前に検査すること	7.2.6	○	固定ハードディスクといった記憶媒体を内蔵している装置は、磁気ディスクを物理的に破壊するか、消磁装置を使用してデータを完全に消去すること。	ファシリティでは、生態認証の情報等を想定している。
				2) 取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアが、消去又は上書きされているか確認	7.2.6	○	重要なデータ及びライセンス供与されたソフトウェアは、消磁装置を使用して消去されているか、上書きされているか確認すること。	
5.3	その他の管理策	情報及び情報処理設備の損傷又は盗難を防止するため	1) 組織は、通常の勤務時間内及び時間外の情報への許可されていないアクセス、情報の消失及び損傷のリスクを軽減するために、書類及び取外し可能な記憶媒体に対するクリアデスク方針の適用、並びに情報処理設	1) クリアデスク及びクリアスクリーンの個別方針において、情報セキュリティの分類に対応するリスクを考慮すること	7.3.1	×		
				2) クリアデスク及びクリアスクリーンの個別方針において、組織の文化的側面を考慮すること	7.3.1	×		
				3) 書類及びコンピュータ媒体は、使用していないとき、特に勤務時間外には、適切に施錠された書庫又は他の形式の安全な収納庫内に保管す	7.3.1	×		
				4) 取扱いに慎重を要する又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して保管しておくこと	7.3.1	×		
				5) パーソナルコンピュータ、コンピュータ端末及び印字装置は、ログオン状態で離席しないこと	7.3.1	×		
				6) パーソナルコンピュータ、コンピュータ端末及び印字装置は、使用しないときは、施錠、パスワード又は他の管理策によって保護すること	7.3.1	×		
				7) 郵便物の受渡し箇所、並びに無人のファクシミリ及びテレックス機を保護すること	7.3.1	×		
				8) 複写機は、通常の勤務時間外は施錠しておく（又は他の何らかの方法によって、認可していない使用から保護する）こと	7.3.1	×		
				9) 取扱いに慎重を要する情報又は機密情報を印刷した場合、印字装置から直ちに取り出すこと	7.3.1	×		
			2) 装置、情報又はソフトウェアは指定場所から無認可ではもち出しできな	1) 持出し時及び返却時に記録を残すこと	7.3.2	×		
				2) 認可されていない資産の移動がおこなわれていないか、現場検査を実施すること	7.3.2	×		
				3) 現場検査があることを各人が認識していること	7.3.2	×		
6.1	運用手順及び責任	情報処理設備の正確、かつ、セキュリティを保った運用を確実にす	1) セキュリティ個別方針によって明確化した操作手順は、文書化して維持し	1) 操作手順は、正式な文書として取り扱うこと	8.1.1	×		ファシリティでは、入退室管理、各種制御系システムを想定。
				2) 操作手順が変更の場合は管理者によって認可されること	8.1.1	×		
				3) 操作手順には、情報の処理及び取扱いを含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				4) 操作手順には、スケジュール作成に関する要求事項を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				5) 操作手順には、作業中に発生し得る誤り又はその他の例外状況の処理についての指示を含む、各作業の詳細な実施に関する指示を明記	8.1.1	×		
				6) 操作手順には、操作上又は技術上の不測の問題が発生した場合の連絡先を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				7) 操作手順には、特別な出力の取扱いに関する指示を含む、各作業の詳細な実施に関する指示を明記す	8.1.1	×		
				8) 操作手順には、システムが故障した場合の再起動及び回復の手順を含む、各作業の詳細な実施に関する指示を明記すること	8.1.1	×		
				9) 情報処理・通信設備に関連するシステムの維持管理活動の手順書を作成すること	8.1.1	×		
			2) 情報処理設備及びシステムの変更について管理すること	1) 情報処理設備及びシステムの変更には正式な管理責任及び手順が定められていること	8.1.2	×		
				2) 運用プログラムは、厳重な変更管理の下に置くこと	8.1.2	○	運用プログラムについては、変更実施者と承認者を分離すること。変更手順、不具合発生時の復帰手順を明確に	
				3) プログラムを変更した場合は、すべての関連情報を含む監査記録を保管すること	8.1.2	○	運用プログラム変更の実施日時、変更内容、手順、変更実施者、承認者、試験結果の記録を保管すること。	
				4) 運用の変更管理と業務用ソフトウェア変更管理との手順を、統合するこ	8.1.2	×		
				5) 重要な変更を識別及び記録すること	8.1.2	○	重要なシステムの変更について管理するため、重要な変更とは何かを定め、変更に関する影響及び承認手順を定	
				6) 重要な変更の潜在的な影響の評価をすること	8.1.2	×		
				7) 変更の申出を正式に承認する手順を確立すること	8.1.2	×		
				8) 変更の詳細の、全関係者への通知をすること	8.1.2	×		
				9) うまくいかない変更を中止すること及び復帰することに対する責任を明確にした手順を確立すること	8.1.2	×		
			3) セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理	1) 情報システムの故障及びサービスの停止に対処できるように、手順を定めること	8.1.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) サービスの妨害（denial of service:DoS）に対処できるように、手順を定めること	8.1.3	×		
				3) 不完全又は不正確な業務データに起因する誤りに対処できるように、手順を定めること	8.1.3	×		
				4) 機密性に対する違反に対処できるように、手順を定めること	8.1.3	×		
				5) 通常の障害対策計画手順には、事件・事故の原因の分析及び識別を	8.1.3	×		
				6) 通常の障害対策計画手順には、再発を防止するための対策の計画及び実施を含めること	8.1.3	×		
				7) 通常の障害対策計画手順には、監査証跡及びこれに類する証拠の収集を含めること	8.1.3	×		
				8) 通常の障害対策計画手順には、事件・事故からの回復に関わる人々への連絡を含めること	8.1.3	×		
				9) 通常の障害対策計画手順には、監督機関に対する措置の報告を含め	8.1.3	×		
				10) 内部問題の分析のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	SYSLOG、ログインログ等ログの収集を行い、アクセス権限を厳重にし、改ざんを防止すること。ログの保管場所は、ログを収集した装置とは別媒体に保管すること。	
				11) 潜在的な契約違反若しくは規制要求事項への違反に関連した証拠、又は、民事若しくは刑事訴訟（例えば、コンピュータの誤用又はデータ保護に関連して制定された法律に基づいたもの）での証拠として使用するために、監査証跡及びこれに類する証拠を収集し、安全に保管する	8.1.3	○	契約違反や規制要求事項に違反した証拠、もしくは訴訟での証拠として使用できるよう、サーバの時刻同期設定を実施すること。ID、入館（入室）、退館（退室）日時を収集すること。収集したログはアクセス権限を厳重にし、改ざんを防止すること。ログの保管場所は、ログを収集した装置とは別媒体に保管すること。	
				12) ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡及びこれに類する証拠を収集し、安全に保管すること	8.1.3	○	ソフトウェア及びサービスの提供者との補償交渉のために、監査証跡として使用できるよう、サーバの時刻同期設定を実施すること。ID、入館（入室）、退館（退室）日時を収集すること。収集したログはアクセス権限を厳重にし、改	
				13) セキュリティ違反からの回復及びシステム故障の修正を行うための措置は、慎重に、かつ、正式に管理さ	8.1.3	×		
				14) 事件・事故管理手順では、身分が明らかで、認可された要員だけに、作動中のシステム及びデータに対するアクセスを、許すことを考慮す	8.1.3	×		
				15) 事件・事故管理手順では、実施したすべての非常措置は、文書に詳細を記録することを考慮すること	8.1.3	×		
				16) 事件・事故管理手順では、非常措置は、経営陣に報告し、手順に従ってレビューを行うことを考慮すること	8.1.3	×		
				17) 事件・事故管理手順では、事業システム及び管理策の完全性を、早急に確認することを考慮すること	8.1.3	×		
			4) 情報若しくはサービスの無認可の変更又は誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理又	1) 職務の分離が困難であれば、活動の監視、監査証跡及び経営者による監督といった他の管理策を考慮すること	8.1.4	×		
				2) セキュリティ監査は、独立性を維持すること	8.1.4	×		
				3) どのような業務でも、誰にも知られずに、単独では不正を働くことができないように注意すること	8.1.4	×		
				4) ある作業を始めることと、その作業を認可することとを分離すること	8.1.4	×		
				5) 不正を働くために共謀が必要となる行動（例えば、購入注文書を作成することと物品の受領を確認すること）は、分離すること	8.1.4	×		
				6) 共謀の恐れがある場合は、二人以上のかかわりが必要となるように管理策を工夫すること	8.1.4	×		
			5) 開発施設、試験施設及び運用施設を分離するため、ソフトウェアの開発から運用の段階への移行についての規則を明	1) 運用環境、試験環境及び開発環境の間で必要となる分離の程度を考慮すること	8.1.5	×		
				2) 同様な分離は、開発と試験との機能間でも実行すること	8.1.5	×		
				3) 意味のある試験を実施し、開発者による不適切なアクセスを防止するために、既知で堅固な環境を維持す	8.1.5	×		
				4) 開発施設、試験施設及び運用施設を分離すること	8.1.5	×		
				5) 開発ソフトウェアと運用ソフトウェアとは、可能ならば、異なるコンピュータで、又は異なる領域若しくはディレクトリで実行すること	8.1.5	×		
				6) 開発作業と試験作業とは、可能な限り分離すること	8.1.5	×		
				7) コンパイラ、エディタ、その他のシステムユーティリティは、必要でない場合、運用システムからアクセスできないこと	8.1.5	×		
				8) 運用システム及び試験システムに対しては、異なるログオン手順を用	8.1.5	×		
				9) 運用システム及び試験システムに対しては、異なるパスワードを使用するように利用者に薦めること	8.1.5	×		
				10) メニューには、適切な識別メッセージを表示すること	8.1.5	×		
				11) 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に運用されている場合にだけ、管理用パスワードを取得す	8.1.5	×		
				12) 管理用パスワードは、使用後には変更されることを確実にすること	8.1.5	×		
			6) 情報処理施設の管理のために外部の請負業者を利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意	1) 外部委託による施設管理においては、取扱いに慎重を要する又は重要で、社内で管理すべき適用業務の識別をすること	8.1.6	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 外部委託による施設管理においては、業務用ソフトウェアの管理者からの承認取得をすること	8.1.6	×		
				3) 外部委託による施設管理においては、事業継続計画との関連性を考	8.1.6	×		
				4) 外部委託による施設管理においては、指定すべきセキュリティ標準類及び適合性の測定手続を考慮する	8.1.6	×		
				5) 外部委託による施設管理においては、関連するすべてのセキュリティ作業を有効に監視するための手順及び責任に関するそれぞれの割当	8.1.6	×		
				6) 外部委託による施設管理においては、セキュリティ事件・事故の報告及び処理についての責任及び手順	8.1.6	×		
6.2	システムの計画作成及び受入れ	システム故障のリスクを最小限に抑えるため	1) 十分な処理能力及び記憶容量が利用できることを確実にするために、容量・能力の需要を監視して、将来必要とされる容	1) 容量・能力の計画の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理における現在の傾向及び予測される傾向を考慮すること	8.2.1	×		・接続サービス：ネットワークトラフィック ・監視サービス：取得するログのディスク容量 等をそれぞれ想定してい
				2) 汎用大型コンピュータによるサービスの管理者は、処理装置、主記憶装置、補助記憶装置、印字装置及びその他の出力装置、並びに通信システムを含む主要なシステム資	8.2.1	×		
				3) 管理者は、使用傾向、特に業務用ソフトウェア又は情報システムの管理ツールと関連した傾向を識別する	8.2.1	×		
				4) システムセキュリティ又は利用者サービスに脅威をもたらす恐れのある潜在的な障害を識別し、その発生を避け、適切な是正の措置を立案するために、管理者は、この情報を	8.2.1	×		
			2) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な試験を	1) 管理者は、新しいシステムを受け入れるための要求事項及び基準を明確に定義すること	8.2.2	×		
				2) 管理者は、新しいシステムを受け入れるための要求事項及び基準を文書化すること	8.2.2	×		
				3) 管理者は、新しいシステムを受け入れるための要求事項及び基準を合意すること	8.2.2	×		
				4) 新しい情報システム、改訂版及び更新版の受入れ基準を確立し、その受入れ前に適切な評価を実施する	8.2.2	×		
				5) 管理者は、新しいシステムを受け入れるための要求事項及び基準を、評価することを確実にすること	8.2.2	×		
				6) システムの受け入れにおいて、性能及びコンピュータの容量・能力の要求事項を考慮すること	8.2.2	×		
				7) システムの受け入れにおいて、誤りからの回復及び再起動の手順並びに障害対策計画を考慮すること	8.2.2	×		
				8) システムの受け入れにおいて、定められた標準類に則った通常の操作手順の準備及び確認を考慮するこ	8.2.2	×		
				9) システムの受け入れにおいて、合意された適切なセキュリティ管理策を考慮すること	8.2.2	×		
				10) システムの受け入れにおいて、手動による有効な手順を考慮すること	8.2.2	×		
				11) システムの受け入れにおいて、事業継続の取決めを考慮すること	8.2.2	×		
				12) システムの受け入れにおいて、月末のような最大処理の時に、新しいシステムを導入することが、既存のシステムに対して悪影響を及ぼさないという証拠について考慮すること	8.2.2	×		
				13) システムの受け入れにおいて、新しいシステムが組織のセキュリティ全般に及ぼす影響について、検討したという証拠を得ること	8.2.2	×		
				14) システムの受け入れにおいて、新しいシステムの運用又は使用に関する訓練を行うこと	8.2.2	×		
				15) 主要な新しいシステム開発においては、設計作業の効率を確保するために、あらゆる段階で運用上の関係者及び利用者から意見を聞くこと	8.2.2	×		
				16) 主要な新しいシステム開発においては、適切な試験を実施し、すべての受入れ基準が完全に満たされていることを確認すること	8.2.2	×		
6.3	悪意のあるソフトウェアからの保護	ソフトウェア及び情報の完全性を保護するため	1) 悪意のあるソフトウェアから保護するための検出及び防止の管理策、並びに利用者に適切に認知させるための手順を導入すること	1) 悪意のあるソフトウェアからの保護は、セキュリティに対する認識、システムへの適切なアクセス、及び変更管理についての管理策に基づくこと	8.3.1	×		ウィルスについては、原則として、ウィルスチェックサービスの対象範囲とし、今回抽出したサービスでは個別に扱わない。ただし、監視サービスについては、監視用端末自体のウィルスチェックを想定したため、範囲に含んでいる
				2) ソフトウェア使用許諾契約の遵守を要求し、無認可のソフトウェアの使用を禁止する組織としての個別方針を考慮すること	8.3.1	×		
				3) 外部ネットワークから若しくは外部ネットワーク経由で、又は他の媒体を通じてファイル及びソフトウェアを入手することによるリスクから保護し、どのような保護対策を行うことが望ましいかを示す組織としての個別	8.3.1	×		
				4) 予防又は定常の作業としてコンピュータ及び媒体を走査するための、ウイルスの検出ソフトウェア及び修復ソフトウェアの導入及び定期	8.3.1	×		
				5) 重要な業務手続を支えるシステムのソフトウェア及びデータの定期的見直しを考慮すること	8.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) 未承認のファイル又は無認可の変更の存在に対しては、正式に調査	8.3.1	×		
				7) 出所の不明確な若しくは無認可の電子媒体上のファイル、又は信頼できないネットワークを通して得たファイルのすべてに対し、ファイル使用前のウイルス検査を考慮すること	8.3.1	×		
				8) 電子メールの添付ファイル及びダウンロードしたファイルのすべてに対し、使用前の悪意のあるソフトウェアの検査を考慮すること	8.3.1	×		
				9) システムのウイルスからの保護、保護策の利用方法に関する訓練を考慮すること	8.3.1	×		
				10) ウイルス感染についての報告、及びウイルス感染からの回復に関する管理の手順及び責任について考	8.3.1	×		
				11) ウイルス感染からの回復のための適切な事業継続計画を考慮するこ	8.3.1	×		
				12) 悪意のあるソフトウェアに関するすべての情報を確認すること	8.3.1	×		
				13) 警告情報が正確、かつ、役立つことを確実にするための手順を考慮す	8.3.1	×		
				14) 管理者は、単なるいたずらと真のウイルスとを識別するために、適切な情報源（例えば、定評のある刊行物、信頼できるインターネットサイト、又はウイルス対策ソフトウェア供給業者）の利用を確実にすること	8.3.1	×		
				15) 職員は、単なるいたずらの問題及びそれらを受け取ったときの対応について認識していること	8.3.1	×		
6.4	システムの維持管理 (Housekeeping)	情報処理及び通信サービスの完全性及び可用性を維持するため	1) 極めて重要な業務情報及びソフトウェアのバックアップは、定期的に取得し、かつ検査すること	1) 災害又は媒体故障が発生した後、極めて重要なすべての業務情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を	8.4.1	×		マシンレンタルサービスのバックアップは、レンタル先のクライアントが原則担当するため、対象外とする。
				2) 最小限のバックアップ情報は、バックアップについての正確及び完全な記録並びに文書化された復元手順とともに、主事業所の災害による損傷を免れることができる十分離れた	8.4.1	×		
				3) 重要な業務用ソフトウェアについては、少なくとも3世代又は3サイクル分のバックアップのための情報を保	8.4.1	×		
				4) バックアップには、主事業所で適用される標準類に従って、適切なレベルの物理的及び環境的保護を施す	8.4.1	×		
				5) 主事業所において媒体に適用する管理策は、バックアップのための事業所に対しても適用すること	8.4.1	×		
				6) 極めて重要な業務情報の保存期間及び永久に保管すべき複製物についてのいかなる要求事項も決定し	8.4.1	×		
				7) バックアップした媒体は、必要な場合の緊急使用のための信頼性を確実とするために、実行可能ならば、定期的に検査すること	8.4.1	×		
				8) 復元手順は、定期的に検査及び試験すること	8.4.1	×		
			2) 運用担当者は、自分の作業の記録を継続すること	1) 記録には、システムの起動及び終了の時刻を含めること	8.4.1	×		
				2) 記録には、システム誤り及び実施した是正処置を含めること	8.4.2	×		
				3) 記録には、データファイル及びコンピュータ出力の正しい取扱いの確認を含めること	8.4.2	×		
				4) 記録には、記録の作成者の名前を含めること	8.4.2	×		
			3) 運用担当者の記録は、定期的に独立した検査を受けること	（なし）	8.4.2	×		
			4) 障害については報告を行い、是正処置をとること	1) 情報処理又は通信システムの問題に関して利用者から報告された障害は、記録すること	8.4.3	×		
				2) 報告された障害の取扱いについては、明確な規定があること	8.4.3	×		
				3) 障害記録規定には、障害が完全に解決したことを確実にするための障害記録の見直しを含むこと	8.4.3	×		
				4) 障害記録規定には、管理策が意味を失っていないこと及び実施された措置が完全に認可されることを確実にするための是正手段の見直しを	8.4.3	×		
6.5	ネットワークの管理	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	1) ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること	1) ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること	8.5.1	×		接続サービスについては、外部および内部のネットワークを想定、また、監視サービスについては、内部
				2) ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にす	8.5.1	×		
				3) ネットワークの運用責任とコンピュータの操作作業とは、適切ならば、分離すること	8.5.1	×		
				4) 遠隔地に所在する設備（利用者の領域におかれた設備を含む）の管理に関する責任及び手順を確立す	8.5.1	×		
				5) 公衆ネットワークを通過するデータの機密性及び完全性を保護するため、及びネットワークに接続したシステムを保護するために、必要ならば、特別な管理策を確立すること	8.5.1	×		
				6) サービスを事業に最大限活用するため、及び管理策を情報処理基盤の全体に一貫して適用することを確実にするために、様々な管理作業を	8.5.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
6.6	媒体の取扱い及びセキュリティ	財産に対する損害及び事業活動に対する妨害を回避するため	1) コンピュータの取外し可能な付属媒体（例えば、テープ、ディスク、カセット）及び印刷された文書の管理手順があること	1) 不要になったことで組織の管理外となる媒体が、再使用可能なものであるときは、それまでの内容を消去すること	8.6.1	×		
				2) 組織の管理外となる媒体のすべてについて、認可を必要とすること	8.6.1	×		
				3) 組織の管理外となる媒体の認可について、監査証跡維持のための記録を保管すること	8.6.1	×		
				4) すべての媒体は、製造者の仕様に従って、安全、かつ、安心できる環境に保管すること	8.6.1	×		
				5) コンピュータの取外し可能な付属媒体の管理に関する、すべての手順及び認可のレベルは、明確に文書	8.6.1	×		
			2) 媒体が不要となった場合は、安全、かつ、確実に	1) 媒体の安全な処分のための、正式な手順を確立すること	8.6.1	×		
				2) 取扱いに慎重を要する情報が記録されている媒体は、安全、かつ、確実に保管すること	8.6.2	×		
				3) 取扱いに慎重を要する情報が記録されている媒体は、更に、安全、かつ、確実に処分するか、又は組織内の別の適用業務で使用するためにデータを消去すること	8.6.2	×		
				4) 十分な管理及び経験がある、書類、装置及び媒体の回収及び処分を行う契約先を選定するために、注意を払うこと	8.6.2	×		
				5) 取扱いに慎重を要する媒体類の処分は、監査証跡を維持するために、可能な方法で記録すること	8.6.2	×		
				6) 処分しようとする媒体を集める場合、集積することによる影響に配慮	8.6.2	×		
			3) 認可されていない露呈又は誤用から情報を保護するために、情報の取扱い及び保管についての手順を確立すること	1) 情報の取扱い手順は、文書、計算処理システム、ネットワーク、移動型計算処理（mobile computing）、移動通信、メール、音声メール、一般の音声通信、マルチメディア、郵便サービス・施設、ファクシミリの使用、他の取扱いに慎重を要するものすべて（例えば、未使用の小切手、送り状）について、その情報の分類	8.6.3	×		
				2) 情報の取扱い手順の策定においては、すべての媒体の取扱い及びラベル付けについて考慮すること	8.6.3	×		
				3) 情報の取扱い手順の策定においては、認可されていない者を識別するためのアクセス制限について考慮	8.6.3	×		
				4) 情報の取扱い手順の策定においては、データの受領者として認可された者の、公式の記録の維持につい	8.6.3	×		
				5) 情報の取扱い手順の策定においては、入力データが完全であること、適切に処理がなされること、及び出力の妥当性の確認がなされることを	8.6.3	×		
				6) 情報の取扱い手順の策定においては、出力待ちのために一時蓄積させたデータの、重要度に応じた保護について考慮すること	8.6.3	×		
				7) 情報の取扱い手順の策定においては、製造者の仕様書に適合した環境での媒体の保管について考慮す	8.6.3	×		
				8) 情報の取扱い手順の策定においては、データの配布先を最小限にすることを考慮すること	8.6.3	×		
				9) 情報の取扱い手順の策定においては、認可された受領者の注意を求めるために、データの複製すべてに行う明確な表示をすることについて	8.6.3	×		
				10) 情報の取扱い手順の策定においては、配布先及び認可された受領者の一覧表の定期的な間隔での見直しについて考慮すること	8.6.3	×		
			4) 認可されていないアクセスからシステムに関する文書を保護すること	1) システムに関する文書は、安全に保管すること	8.6.4	×		
				2) システムに関する文書にアクセスできる者は、人数を最小限に抑えるこ	8.6.4	×		
				3) システムに関する文書にアクセスできる者は、当該業務の管理者によって認可されること	8.6.4	×		
				4) システムに関する文書で、公衆ネットワークの公衆ネットワークの中で保持されるもの、又は公衆ネットワーク経由で提供されるものは、適切に保護すること	8.6.4	×		
6.7	情報及びソフトウェアの交換	組織間で交換される情報の紛失、改ざん又は誤用を防止するため	1) 組織間の情報及びソフトウェアの交換（電子的又は人手によるもの）については、ある場合には正式な契約として、合意を取り交わすこと	1) 情報及びソフトウェアの交換契約の合意におけるセキュリティの扱いには、関連する業務情報の重要度を反映させること	8.7.1	×		
				2) セキュリティ条件にかかわる合意では、送信、発送及び受領の管理、及びそれらの通知を行う管理者の責任について考慮すること	8.7.1	×		
				3) セキュリティ条件にかかわる合意では、送主、送信、発送及び受領を通知する手順について考慮すること	8.7.1	×		
				4) セキュリティ条件にかかわる合意では、梱包及び送信に関する必要最小限の技術基準標準を考慮するこ	8.7.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) セキュリティ条件にかかわる合意では、配送者の身分を確認する基準標準について考慮すること	8.7.1	×		
				6) セキュリティ条件にかかわる合意では、データが紛失したときの責任及び保証について考慮すること	8.7.1	×		
				7) セキュリティ条件にかかわる合意では、取扱いに慎重を要する又は重要な情報に関する合意されたラベル付けシステムの使用について考	8.7.1	×		
				8) セキュリティ条件にかかわる合意では、情報・ソフトウェアの管理権、及びデータ保護、ソフトウェアの著作権の遵守、その他のこれに類する考慮事項に対する責任について考	8.7.1	×		
				9) セキュリティ条件にかかわる合意では、情報・ソフトウェアの記録及び読出しに関する技術標準について考	8.7.1	×		
				10) セキュリティ条件にかかわる合意では、取扱いに慎重を要するもの（例えば、暗号かぎ）を保護するために必要とされる特別な管理策を考慮	8.7.1	×		
			2) 配送されるコンピュータ媒体を、認可されていないアクセス、誤用又は破損から保護すること	1) 媒体の配送においては、すべての認可された宅配業者について管理者の合意を得ること	8.7.2	×		
				2) 媒体の配送においては、信頼できる輸送機関又は宅配業者を用いるこ	8.7.2	×		
				3) 媒体の配送においては、宅配業者の身分を確認する手順を導入する	8.7.2	×		
				4) 製造者の仕様に従い、梱包を、配送途中に生じるかも知れない物理的損傷から内容物を保護するのに十分な強度とすること	8.7.2	×		
				5) 媒体の配送においては、施錠されたコンテナの使用を考慮すること	8.7.2	×		
				6) 媒体の配送においては、手渡しを考慮すること	8.7.2	×		
				7) 媒体の配送においては、開封防止包装の利用を考慮すること	8.7.2	×		
				8) 媒体の配送においては、特別な場合には、貨物を複数に分け、異なる経路での配送を考慮すること	8.7.2	×		
				9) 媒体の配送においては、ディジタル署名及び秘匿のための暗号の使用を考慮すること	8.7.2	×		
			3) 電子商取引を、不正行為、契約紛争、及び情報の露呈又は改ざんから保護すること	1) 電子商取引のセキュリティにおいては、認証（買い手及び売り手はそれぞれが主張している自らの身分について、どの程度の信頼を要求す	8.7.3	×		
				2) 電子商取引のセキュリティにおいては、認可（価格を決める権限、重要な取引文書を発行する権限又は重要な取引文書に署名する権限は誰にあるか、取引相手はこれらをどう	8.7.3	×		
				3) 電子商取引のセキュリティにおいては、契約及びその申込手続について考慮すること	8.7.3	×		
				4) 電子商取引のセキュリティにおいては、価格情報について考慮すること	8.7.3	×		
				5) 電子商取引のセキュリティにおいては、注文取引について考慮すること	8.7.3	×		
				6) 電子商取引のセキュリティにおいては、審査について考慮すること	8.7.3	×		
				7) 電子商取引のセキュリティにおいては、決済について考慮すること	8.7.3	×		
				8) 電子商取引のセキュリティにおいては、注文について考慮すること	8.7.3	×		
				9) 電子商取引のセキュリティにおいては、責任について考慮すること	8.7.3	×		
				10) 電子商取引に関する当事者間の合意は、権限の詳細も含め、合意した取引条件を両当事者に義務付ける契約書によって裏付けること	8.7.3	×		
				11) 情報サービス事業者と付加価値ネットワーク事業者との間にも、合意を交わすこと	8.7.3	×		
				12) 公開している取引システムでは、その取引条件を顧客に公表すること	8.7.3	×		
				13) 電子商取引に用いる基幹コンピュータのもつ攻撃に対する耐性について、及び電子商取引の実施に必要なネットワーク相互接続のセキュリティ上のかかわりについて、	8.7.3	×		
			4) 電子メールにおけるセキュリティ上のリスクを軽減するための管理策の必要性について考慮す	1) 電子メールの使用に関しての個別方針には、電子メールに対する攻撃の対処を含めること	8.7.4.1	×		マシンレンタルサービスは、貸し出しサーバ上でクライアントが電子メールを利用する場合を想定。
				2) 電子メールの使用に関しての個別方針には、電子メールの添付ファイルの保護を含めること	8.7.4.2	×		監視サービスについては、障害発生等の連絡を対象となる担当者へ連絡する際
				3) 電子メールの使用に関しての個別方針には、電子メールを使うべきでないときに関する指針を含めること	8.7.4.2	×		
				4) 電子メールの使用に関しての個別方針には、会社の信用を傷つける恐れのある行為に対する従業員の	8.7.4.2	×		
				5) 電子メールの使用に関しての個別方針には、電子メッセージの機密性及び完全性を保護するための、暗号技術の利用を含めること	8.7.4.2	×		
				6) 電子メールの使用に関しての個別方針には、保管していれば訴訟の場合証拠として使える可能性があるメッセージの保存を含めること	8.7.4.2	×		
				7) 電子メールの使用に関しての個別方針には、認証できなかったメッセージ交換を調査するための追加の管理策を含めること	8.7.4.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			5) 電子オフィスシステムに関連する業務上及びセキュリティ上のリスクを管理するために、個別方針	1) 電子オフィスシステムのセキュリティにおいては、オフィスシステムにおける情報のぜい(脆)弱性を考慮すること	8.7.5	×		電子オフィスシステムは、監視サービスにおける定期レポート作成の際に使用することを想定。
				2) 電子オフィスシステムのセキュリティにおいては、情報の共有を管理するための、個別方針及び適切な管理策について考慮すること	8.7.5	×		
				3) 電子オフィスシステムのセキュリティにおいては、システムが適切な水準の保護を提供しない場合は、取扱いに慎重を要する業務情報の分類区分を除外すること	8.7.5	×		
				4) 電子オフィスシステムのセキュリティにおいては、特別の人（例えば、重要な業務計画に従事している職員）が関係する業務日誌へのアクセスを制限することを考慮すること	8.7.5	×		
				5) 電子オフィスシステムのセキュリティにおいては、業務処理（例えば、通信の手順、通信の認可）を支えているシステムの適合性などについて	8.7.5	×		
				6) 電子オフィスシステムのセキュリティにおいては、システムの使用を許可された職員、請負業者又は提携業者の区分、システムにアクセスすることが許される場所について考慮す	8.7.5	×		
				7) 電子オフィスシステムのセキュリティにおいては、特別の設備に対するアクセスを特定の区分に属する利用者に限定することを考慮すること	8.7.5	×		
				8) 電子オフィスシステムのセキュリティにおいては、利用者の地位の識別を考慮すること	8.7.5	×		
				9) 電子オフィスシステムのセキュリティにおいては、システムがもっている情報の保持及びバックアップについて考慮すること	8.7.5	×		
				10) 電子オフィスシステムのセキュリティにおいては、緊急時に用いる代替手段についての要求事項及び取決めについて考慮すること	8.7.5	×		
			6) 電子的に公開した情報の完全性を保護するように注意すること	1) 公開されたシステム（例えば、インターネット経由でアクセスできるウェブサーバ）に掲載している情報は、システムが設置された地域又は取引が行われている地域に適用される、法律、規則及び規制に適合する	8.7.5	×		
				2) 情報を公開する前に、正式な認可の手続がとられること	8.7.6	×		
				3) 高い水準での完全性を要求する、ソフトウェア、データ、その他の情報を、公開しているシステムの上で使用できるようにした場合は、ディジタル署名などの適切な手段によって	8.7.6	×		
				4) 公開している電子システムは、それが情報のフィードバック及び直接入力を許すものである場合には、情報は、あらゆるデータ保護に関連して制定された法律に従って収集するこ	8.7.6	×		
				5) 公開のシステムに入力し、そこで処理する情報は、遅滞なく、完全、かつ、正確に、処理すること	8.7.6	×		
				6) 取扱いに慎重を要する情報は、収集の過程及び保管時に保護するこ	8.7.6	×		
				7) 公開のシステムにアクセスができても、アクセス権限がないと先のネットワークへのアクセスは、許さないこ	8.7.6	×		
			7) 音声・映像の通信設備及びファクシミリを使用して行われる情報交換を保護するために、適切な	1) 音声・画像通信設備及びファクシミリを使用するときに職員が従うべき手順についての明確な個別方針文書を策定すること	8.7.7	×		
				2) 電話を使うときには、適切な注意を払うことの必要を、職員に意識させること	8.7.7	×		
				3) 職員に、一般の場所又は出入り自由のオフィス及び壁が薄い会議室で、機密の会話をしないようにさせ	8.7.7	×		
				4) 留守番電話には、認可されていない者による再生、共用機器での録音、又は電話番号を間違ってダイヤルすることの結果として間違い録音の恐れがあるので、メッセージを残	8.7.7	×		
				5) 職員に、ファクシミリを用いる上での問題点を意識させること	8.7.7	×		
7.1	アクセス制御に関する業務上の要求事項	情報へのアクセス制御をするため	1) アクセス制御についての業務上の要求事項を定義し、文書化すること	1) 利用者ごと、または利用者からなるグループごとに対するアクセス制御規則を、アクセス方針宣言書に明確に記述すること	9.1.1.1	×		
				2) 利用者ごと、または利用者からなるグループごとに対するアクセス権を、アクセス方針宣言書に明確に記述すること	9.1.1.1	×		
				3) 利用者及びサービス提供者には、アクセス制御によって満たされるべき業務上の要求事項の明確な宣言書を与えること	9.1.1.1	×		
				4) アクセス制御に関する個別方針には、個々の業務用ソフトウェアのセキュリティ要求事項を考慮すること	9.1.1.1	×		
				5) アクセス制御に関する個別方針には、業務用ソフトウェアに関わるすべての情報の識別を考慮すること	9.1.1.1	×		
				6) アクセス制御に関する個別方針には、情報の伝達及びアクセスの認可に対する個別方針（例えば、情報を知る必要がある要因の選定基準、情報のセキュリティ水準の設定基準、情報の分類基準）を考慮する	9.1.1.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				7) アクセス制御に関する個別方針には、異なるシステム及びネットワークにおける、アクセス制御と情報分類の方針との整合性を考慮すること	9.1.1.1	×		
				8) アクセス制御に関する個別方針には、データ又はサービスへのアクセスの保護に関連する関連法令及び契約上の義務を考慮すること	9.1.1.1	×		
				9) アクセス制御に関する個別方針には、一般的な職務区分に対する標準的な利用者のアクセス権限情報を考慮すること	9.1.1.1	×		
				10) アクセス制御に関する個別方針には、使用可能な全接続形態を認識する分散ネットワーク環境におけるアクセス権の管理を考慮すること	9.1.1.1	×		
				11) アクセス制御の規則を定める際は、常に遵守しなければならない規則と選択的又は条件付規則とを区別す	9.1.1.2	×		
				12) アクセス制御の規則を定める際は、"明確に禁止していなければ原則的に許可する"という前提に基づいた弱い規則よりも、"明確に許可していなければ原則的に禁止する"という前提に基づいた規則を設定す	9.1.1.2	○	アクセス権限の規則を定める際は、アクセス権限のデフォルトをアクセス不可とし、必要な作業内容に応じて権限を改めて付与すること。	
				13) アクセス制御の規則を定める際は、情報処理設備によって自動的に初期設定される情報ラベルの変更、及び利用者の判断によって初期設定される情報ラベルの変更をするこ	9.1.1.2	○	アクセス権限の規則を定める際は、アクセス権限のデフォルトをアクセス不可とし、必要な作業内容に応じて権限を改めて付与すること。	
				14) アクセス制御の規則を定める際は、情報システムによって自動的に初期設定される利用者のアクセス許可の変更、及び管理者によって初期設定される利用者のアクセス権の変更をすること	9.1.1.2	○	アクセス権限の規則を定める際は、管理者は、アクセス権限のデフォルトをアクセス不可とし、必要な作業内容に応じて権限を改めて付与すること。	
				15) アクセス制御の規則を定める際は、設定前に管理者又はその他の承認を必要とする規則とそのような承認を必要としない規則との区別をする	9.1.1.2	×		
7.2	利用者のアクセス管理	情報システムへの認可されていないアクセスを防止するため	1) 複数の利用者をもつすべての情報システム及びサービスについて、それらへのアクセスを許可するための、正規の利用者登録及び登録削除の手続があること	1) 複数の利用者をもつ情報サービスへのアクセスは、正式な利用者登録手続によって管理すること	9.2.1	×		
				2) 利用者登録手続において、利用者との対応付けができ、また、利用者に自分の行動に責任を負わせることができるように、一意な利用者IDを用いること	9.2.1	×		
				3) 利用者登録手続において、グループIDの使用は、実施される作業に適切な場合にだけ許可すること	9.2.1	×		
				4) 利用者登録手続において、利用者が情報システム又はサービスの使用に対して、システムの実務管理者から認可を得ているかを検査するこ	9.2.1	×		
				5) 利用者登録手続において、許可されているアクセスのレベルが、業務の目的に適しているかを検査するこ	9.2.1	×		
				6) 利用者登録手続において、組織のセキュリティ基本方針と整合しているか（例えば、職務権限の分離に矛盾する恐れはないか）を検査するこ	9.2.1	○	利用者IDに付与された権限は、業務上必要な権限に限定されているか検査すること。	
				7) 利用者登録手続において、重複する利用者IDが別の利用者に発行されないことを確実にすること	9.2.1	○	利用者IDは、社員番号等一意の番号と連動させ、重複の照合を行うこと。	
				8) 利用者登録手続において、職員又はサービス業者が認可されていないアクセスを試みた場合の処罰を明記する条項を、職員契約及びサービス契約に含めることを考慮す	9.2.1	×		
				9) 利用者登録手続において、アクセス権の宣言書を利用者に発行するこ	9.2.1	×		
				10) 利用者登録手続において、アクセスの条件を理解していることを示している宣言書への署名を利用者に要求すること	9.2.1	×		
				11) 利用者登録手続において、認可手続が完了するまでサービス提供者が利用者にアクセスさせないように	9.2.1	×		
				12) 利用者登録手続において、サービスを使用するために登録されているすべての人の正規の記録を維持管理すること	9.2.1	×		
				13) 利用者登録手続において、職務を変更した利用者、又は組織から離れた利用者のアクセス権を直ちに取り消すこと	9.2.1	×		
				14) 利用者登録手続において、もはや必要のない利用者ID及びアカウントがないか定期的に検査し、あれば削除すること	9.2.1	×		
			2) 特権の割り当て及び使用は、制限し、管理すること	1) 認可されていないアクセスに対する保護が必要なものには、正規の認可手続によって特権の割当てを管理すること	9.2.2	×		
				2) 各システム製品に関連した特権と特権が割り当てられる必要がある業務区分に関連した特権とを識別	9.2.2	×		
				3) 個人に対する特権は、使用の必要性に基づき、また、事象ごとに、すなわち、必要とされる場合に限って、その機能上の役割の最小限の要求事項に従って、割り当てること	9.2.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 特権の割り当てにおいて、特権は、認可手続が完了するまで、許可しないこと	9.2.2	○	特権の割り当てにおいて、特権の設定作業者と別の承認者が確認を行い、認可を受けてから使用可能の通知をすること。	
				5) 特権の割り当てにおいて、利用者に対する特権の許可が必要ないように、システムルーチンの開発及び使用を促進すること	9.2.2	×		
				6) 特権の割り当てにおいて、特権は、通常の業務用途に使用される利用者IDとは別の利用者IDに、割り当て	9.2.2	○	特権の割り当ては、通常利用される利用者IDとは兼用せず、新たに別IDを割り上てること。	
			3) パスワードの割当ては、正規の管理手続によって統制すること	1) パスワード管理手続の取組において、個人のパスワードを秘密に保つこと	9.2.3	×		
				2) パスワード管理手続の取組において、グループのパスワードはグループのメンバー内だけの秘密に保つ旨の宣言書への署名を、利用者に	9.2.3	×		
				3) パスワード管理手続の取組において、利用者が自分自身のパスワードを維持管理することが必要な場合、直ちに変更が強制される安全な仮のパスワードが最初に発行されることを確実にすること	9.2.3	○	パスワードの付与において、利用者が最初にログオンする際にパスワード変更を強制される、仮パスワード発行機能を採用すること。	
				4) パスワード管理手続の取組において、利用者がパスワードを忘れた場合に発行される仮のパスワードは、利用者の確実な身分証明がなされた後にだけ発行されること	9.2.3	×		
				5) パスワード管理手続の取組において、セキュリティが保たれた方法で仮のパスワードが利用者に与えられることを要求すること	9.2.3	×		
				6) パスワード管理手続の取組において、第三者の介在又は保護されていない（暗号化されていない）電子メールのメッセージの使用は、避け	9.2.3	×		
				7) パスワード管理手続の取組において、利用者は、パスワードの受領を知らせること	9.2.3	×		
				8) パスワード管理手続の取組において、パスワードは、コンピュータシステムに、保護されていない状態では決して保存しないこと	9.2.3	○	パスワード情報には暗号化を行い、パスワードリストへのアクセスを制限すること。	
				9) パスワード管理手続の取組において、利用者の識別及び認証のためのその他の技術（例えば、指紋の検証、手書き署名の検証などの生体認証、及びICカードなどのハードウェアトークンの使用）も使用可能であり、適切ならば、それらも考慮	9.2.3	○	利用者の識別及び認証のため、カード（スマートカード、磁気カード、近接型カード）や生体認証（指紋、虹彩、網膜、筆跡、音声、掌形等）の使用を検討すること。	
			4) データ及び情報サービスへのアクセスに対する有効な管理を維持するため、経営陣は、利用者のアクセス権を見直す正規の手順を、定期的に実施すること	1) 利用者アクセス権の見直しにおいて、利用者のアクセス権を定期的に、また、何か変更があった後に見直すこと	9.2.4	×		
				2) 利用者アクセス権の見直しにおいて、特権的アクセス権の認可は、更に多い頻度で見直すこと	9.2.4	×		
				3) 利用者アクセス権の見直しにおいて、特権の割当てを定期的に検査して、認可されていない特権が取得されてないことを確実にすること	9.2.4	×		
7.3	利用者の責任	認可されていない利用者のアクセスを防止するため	1) 利用者は、パスワードの選択及び使用に際して、正しいセキュリティ慣行に従うこと	1) すべての利用者に、パスワードを秘密にしておくように助言すること	9.3.1	×		
				2) すべての利用者に、パスワードを紙に記録して保管しないように助言すること	9.3.1	×		
				3) すべての利用者に、システム又はパスワードに対する危険の兆候が見られる場合は、パスワードを変更するように助言すること	9.3.1	×		
				4) すべての利用者に、最短6文字の質の良いパスワードを選択すること	9.3.1	×		
				5) すべての利用者に、パスワードは定期的に、又はアクセス回数に基づいて変更するように助言すること	9.3.1	×		
				6) すべての利用者に、特権アカウントのパスワードは、通常のパスワードより頻繁に変更するように助言する	9.3.1	×		
				7) すべての利用者に、古いパスワードを再使用したり、循環させて使用したりしないように助言すること	9.3.1	×		
				8) すべての利用者に、仮のパスワードは、最初のログオン時点で変更するように助言すること	9.3.1	×		
				9) すべての利用者に、自動ログオン処理にパスワードを含めないように助言すること	9.3.1	×		
				10) すべての利用者に、個人用のパスワードを共有しないように助言する	9.3.1	×		
				11) すべての利用者に、利用者が複数のサービス又はプラットフォームにアクセスする必要があって、複数のパスワードを維持することが要求される場合、そのサービスが保管したパスワードを適切に保護しているときは、利用者は一つの質の良いパスワードを用いてもよいことを助言	9.3.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
			2) 無人運転の装置の利用者は無人運転の装置が適切な保護対策を備えていることを確実にすること	1) 無人運転の装置が利用者の作業領域に取り付けられている装置（例えば、ワークステーション、ファイルサーバ）は、長期間無人のまま放置される場合、認可されていないアクセスからの特別な保護すること	9.3.2	○	居室に長時間無人のまま放置されるシステムコンソールは、ログインしたまま放置しないようにすること。離席時には、パスワード付スクリーンセーバの利用、もしくはログオフを実施すること。	
				2) 無人運転の装置の保護を実施する責任と同様に、その装置を保護するためのセキュリティ要求事項及び手順についても、すべての利用者及び請負業者に認識させること	9.3.2	×		
				3) 無人運転の装置の利用者に、実行していた処理（session）が終わった時点で、接続を切るように助言すること	9.3.2	×		
				4) 無人運転の装置の利用者に、処理（session）が終了したら、汎用大型コンピュータをログオフするように助言すること	9.3.2	×		
				5) 無人運転の装置の利用者に、パーソナルコンピュータ又は端末装置は、使用していない場合、キーロック又は同等の管理策（例えば、パスワードアクセス）によって認可されていない使用からセキュリティを保つように保護するように助言すること	9.3.2	×		
7.4	ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	1) 利用者には、ネットワークサービスへのセキュリティが確保されていない接続は、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること	1) ネットワーク及びネットワークサービスの使用に関し、個別方針を明確に設定すること	9.4.1	×		
				2) ネットワークサービスの使用についての個別方針には、アクセスすることが許されるネットワーク及びネットワークサービスを対象にすること	9.4.1	×		
				3) ネットワークサービスの使用についての個別方針には、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にすること	9.4.1	×		
				4) ネットワークサービスの使用についての個別方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための管理策及び管理手順を対象にすること	9.4.1	×		
				5) ネットワークサービスの使用についての個別方針には、業務上のアクセス制御方針と整合していること	9.4.1	×		
			2) 利用者端末と利用者がアクセスすることを認可されているサービスとの間に、指定された経路以外の経路を、利用者が選択することを防止する	1) 指定された経路以外の経路を、利用者が選択することを防止するために、通常、経路の異なる接続点において幾つかの制御を実施すること	9.4.2	×		
				2) 指定された接続経路には、専用線又は専用電話番号を割り当てること	9.4.2	×		
				3) 指定された接続経路では、指定された業務システム又はセキュリティゲートウェイのポートに自動接続すること	9.4.2	×		
				4) 指定された接続経路では、個々の利用者のためのメニュー及びサブメニューの選択できる内容を制限すること	9.4.2	×		
				5) 指定された接続経路では、ネットワーク上で無制限に探索（roaming）することを防止すること	9.4.2	×		
				6) 指定された接続経路では、外部のネットワーク利用者には、指定された業務システム及び/又はセキュリティゲートウェイを使用させること	9.4.2	×		
				7) 指定された接続経路では、送信元とその送信元に許された送信相手との通信を、セキュリティゲートウェイ（例えば、ファイアウォール）経由で、能動的に制御すること	9.4.2	×		
				8) 組織内の利用者グループのために別々の論理領域[例えば、仮想私設網（Virtual Private Network：VPN）]を設定することによって、ネットワークアクセスを制限すること	9.4.2	×		
				9) 経路を指定することに関する要求事項は、業務上のアクセス制御方針に基づくこと	9.4.2	×		
			3) 遠隔地からの利用者のアクセスには、認証を行うこと	1) コールバックの手順及び制御を用いるとき、組織は、転送機能をもつネットワークサービスを用いないこと	9.4.3	×		
				2) 転送機能をもつネットワークサービスを用いる場合、転送にかかわる弱点を避けるために、この機能の使用を禁止すること	9.4.3	×		
				3) コールバックの手順及び制御を徹底的に試験すること	9.4.3	×		
			4) 遠隔コンピュータシステムへの接続は、認証されること	（なし）	9.4.4	×		
			5) 診断ポートへのアクセスは、セキュリティを保つように制御されること	1) 診断ポートは、適切なセキュリティ機構（例えば、キーロック）、及びコンピュータサービスの管理者とアクセスを必要とするハードウェア・ソフトウェアの支援要員との間の取決めに基づく場合にだけ、それらのポートがアクセス可能であることを確実にする手順によって保護されること	9.4.5	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				2) ネットワークサービスを使用する組織は、使用するすべてのサービスのセキュリティの特質について、明確な説明を受けることを確実にする	9.4.5	×		
			6) 情報サービス、利用者及び情報システムのグループを分割するために、ネットワーク内に制御の導入を考慮すること	1) 相互に接続する二つのネットワーク間にセキュリティゲートウェイは、これらの領域間の通信をフィルタにかけ、また、組織のアクセス制御方針に従って認可されていないアクセスを阻止するように構成すること	9.4.6	×		
				2) ネットワークを幾つかの領域に分離する基準は、アクセス制御方針及びアクセス要求事項に基づくこと	9.4.6	×		
				3) 適切なネットワークの経路指定又はセキュリティゲートウェイ技術を組み込むことの、費用対効果を考慮する	9.4.6	×		
			7) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に基づくこと	1) 利用者の接続の可能性を制限する制御策は、業務用ソフトウェアのアクセス方針及び要求事項に従って維持及び更新されること	9.4.7	×		
				2) 電子メールには制限を適用すること	9.4.7	×		
				3) 一方向のファイル転送には制限を適用すること	9.4.7	×		
				4) 双方向のファイル転送には制限を適用すること	9.4.7	×		
				5) 対話型アクセスには制限を適用すること	9.4.7	×		
				6) 時間帯又は日付に対応したネットワークアクセスには制限を適用する	9.4.7	×		
			8) 共用ネットワーク、特に、組織の境界を越えて広がっているネットワークには、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために、経路指定の制御策を組み込むこと	1) 経路指定の制御は、発信元及びあて先のアドレスを能動的に検査する機構に基づくものであること	9.4.8	×		
				2) ソフトウェア又はハードウェアによって実施されるネットワークアドレスの変換の実施者は、組み込まれた機構の強度を認識しておくこと	9.4.8	×		
			9) ネットワークを使用する組織は、使用するサービスのセキュリティの特質について、明確な説明を受けることを確実にする	（なし）	9.4.9	×		
7.5	オペレーティングシステムのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) 特定の場所及び携帯装置への接続を認証するために、自動の端末識別を考慮すること	（なし）	9.5.1	×		
			2) 情報サービスへのアクセスは、安全なログオン手続を経て達成されること	1) コンピュータシステムへログインするための手順は、認可されていないアクセスの恐れを最小限に抑えるように設計すること	9.5.2	○		
				2) システムについての情報の開示は最小限にすること	9.5.2	○		
				3) ログオン手順は、システム又は業務用ソフトウェアの識別子を、ログオン手続が無事完了するまで表示しな	9.5.2	○		
				4) ログオン手順は、コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示するこ	9.5.2	○		
				5) ログオン手順中に、認可されていない利用者の助けとなる表示をしない	9.5.2	○		
				6) 誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しないこ	9.5.2	○		
				7) 許容されるログオンの試みの失敗回数を制限すること	9.5.2	○		
				8) ログオンの失敗時には、次のログオンの試みが可能となるまでの間に意図的な時間をおくこと	9.5.2	○		
				9) ログオンの失敗時には、特別な認可なしに行われる次回の試みを拒否すること	9.5.2	○		
				10) ログオンの失敗時には、データリンク接続を切ること	9.5.2	○		
				11) ログオン手順のために許容される最長時間及び最短時間を制限する	9.5.2	○		
				12) 許容される最長時間及び最短時間の制限から外れる場合、システムはログオンを終了すること	9.5.2	○		
				13) ログオンの失敗時には、失敗した試みを記録すること	9.5.2	○		
				14) ログオンが無事できた時点で、前回ログオンが無事できた日時を表示すること	9.5.2	○		
				15) ログオンが無事できた時点で、前回のログオン以降、失敗したログオンの試みがある場合は、その詳細を表示すること	9.5.2	○		
			3) すべての利用者（技術支援要員、例えば、オペレータ、ネットワーク管理者、システムプログラマ、データベース管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（利用者ID）を保有	1) 利用者IDには、利用者の特権レベル[例えば、管理者(マネージャ)、監督者(スーパーバイザ)]を表示しないこと	9.5.3	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 明らかに業務上の利点がある例外的状況において、利用者のグループ又は特定の業務に対して、共有利用者IDを用いる場合、管理者の承認を文書で得ること	9.5.3	×		
			4) 質のよいパスワードであることを確実にするために、パスワード管理システムは有効な対話的機能を提供すること	1) パスワードの管理システムでは、責任の所在を明確にするために、利用者本人のパスワードを使用させること	9.5.4	○		
				2) パスワードの管理システムでは、適切ならば、利用者に自分のパスワードの選択及び変更を許可し、入力誤りを考慮した確認手順を組み	9.5.4	○		
				3) パスワードの管理システムでは、質の良いパスワードを選択させるようにすること	9.5.4	○		
				4) パスワードの管理システムでは、利用者が自分のパスワードを維持管理する場合、定期的にパスワードを変更させるようにすること	9.5.4	○		
				5) パスワードの管理システムでは、利用者がパスワードを選択する場合、仮のパスワードは最初のログオン時に変更させるようにすること	9.5.4	○		
				6) パスワードの管理システムでは、以前の利用者パスワードの記録を、一定期間、維持し再使用を防止す	9.5.4	○		
				7) パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにすること	9.5.4	○		
				8) パスワードの管理システムでは、パスワードのファイルは、業務用システムのデータとは別に保存すること	9.5.4	○		
				9) パスワードの管理システムでは、一方向性暗号アルゴリズムを用いて、暗号化した形でパスワードを保存す	9.5.4	○		
				10) パスワードの管理システムでは、ソフトウェアを導入した後は、製造者が初期値（default）として設定したパスワードをすぐに変更すること	9.5.4	○		
			5) システムユーティリティのために認証手順を使用すること	1) 業務用ソフトウェアからシステムユーティリティを分離すること	9.5.5	×		
				2) システムユーティリティの使用を、可能な限り少人数の信頼できる認可された利用者だけに制限すること	9.5.5	×		
				3) システムユーティリティを臨時に使用する際には認可をすること	9.5.5	×		
				4) システムユーティリティの使用の制限をすること	9.5.5	×		
				5) システムユーティリティのすべての使用を記録すること	9.5.5	×		
				6) システムユーティリティの認可レベルの明確化及び文書化をすること	9.5.5	×		
				7) すべての不要なユーティリティソフトウェア及びシステムソフトウェアの除去をすること	9.5.5	×		
			6) 脅迫の標的となり得る利用者のために、脅迫に対する警報(duress alarm)を備えることを考慮する	1) 脅迫に対する警報を備えるかどうかの決定は、リスクの評価に基づくこと	9.5.6	×		
				2) 脅迫に対する警報に対応する責任及び手順を明確に定めること	9.5.6	×		
			7) リスクの高い場所（例えば、組織のセキュリティ管理外にある公共又は外部領域）にあるか、又はリスクの高いシステムで用いられている端末が活動停止状態にある場合、一定の活動停止時間の経過後、その端末	1) 端末のタイムアウト機能は、一定の活動停止時間の経過後、端末の画面を閉じ、業務用ソフトウェアとネットワーク接続とを共に閉じるものであること	9.5.7	×		
				2) 端末のタイムアウト機能までの時間は、端末の領域及び利用者のセキュリティリスクを反映するものであ	9.5.7	×		
			8) リスクの高い業務用ソフトウェアに対して、接続時間の制限によって、追加のセキュリティを提供	1) 既定の時間枠（例えば、バッチファイル伝送のための時間枠）を使うか、又は短時間の通常の対話型処理（session）を用いること	9.5.8	×		
				2) 残業時間又は延長時間の運転の要求がない場合、接続時間を通常の就業時間に制限すること	9.5.8	×		
7.6	業務用ソフトウェアのアクセス制御	認可されていないコンピュータアクセスを防止するため	1) ソフトウェア及び情報への論理アクセスは、認可されている利用者に制限されること	1) 支援要員を含め、業務用システムの利用者は、既定のアクセス制御方針に従い、個々の業務用ソフトウェアの要求事項に基づき、また、組織の情報アクセス方針に合わせて、情報及び業務用システム機能へのアクセスを許されること	9.6.1	○		
				2) 情報へのアクセス制限では、業務用システム機能へのアクセスを制御するための情報の表示を考慮す	9.6.1	○		
				3) 情報へのアクセス制限では、利用者向けの文書を適切に編集して、アクセスを認可されていない情報又は業務用システム機能に関する利用者の知識を限定することを考慮	9.6.1	×		
				4) 情報へのアクセス制限では、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御することを考慮すること	9.6.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) 情報へのアクセス制限では、取扱いに慎重を要する情報を処理する業務用システムからの出力は、その出力の使用に関連し、かつ、認可されている端末及び場所にだけ送られる情報だけを含むことを確実にす	9.6.1	○		
				6) 情報へのアクセス制限では、その出力に対して余分な情報を取り除くことを確実にするために、このような出力の定期的な見直しも行うことを考慮すること	9.6.1	○		
			2) 取扱いに慎重を要するシステムには、専用の隔離された情報システムを設置すること	1) 業務用システムの取扱いに慎重を要する度合は、業務用ソフトウェアの管理者によって明確に識別され、文書化されること	9.6.2	×		
				2) 取扱いに慎重を要する業務用プログラムを共有環境で実行する場合は、資源を共有する業務用システムを識別して、そのプログラムの管理者の合意を得ること	9.6.2	×		
7.7	システムアクセス及びシステム使用状況の監視	認可されていない活動を検出するため	1) 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査及びアクセス制御の監視を補うために、合意された期間保存すること	1) 監査記録には、利用者IDを含めること	9.7.1	○		
				2) 監査記録には、ログオン及びログオフの日時を含めること	9.7.1	○		
				3) 監査記録には、可能ならば、端末のID又は所在地を含めること	9.7.1	○		
				4) 監査記録には、システムへのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○		
				5) 監査記録には、データ、他の資源へのアクセスを試みて、成功及び失敗した記録を含めること	9.7.1	○		
			2) 情報処理設備の使用状況を監視する手順を確立すること	1) 個々の設備に対して要求される監視レベルは、リスクアセスメントによって決めること	9.7.2.1	○		
				2) 監視項目には、認可されているアクセスについて、利用者IDを含むこと	9.7.2.1	○		
				3) 監視項目には、認可されているアクセスについて、その重要な事象の日時を含むこと	9.7.2.1	○		
				4) 監視項目には、認可されているアクセスについて、その事象のタイプを含むこと	9.7.2.1	○		
				5) 監視項目には、認可されているアクセスについて、アクセスされたファイルを含むこと	9.7.2.1	○		
				6) 監視項目には、認可されているアクセスについて、使用されたプログラム・ユーティリティを含むこと	9.7.2.1	○		
				7) 監視項目には、すべての特権操作について、監督者アカウントの使用の有無を含めること	9.7.2.1	○		
				8) 監視項目には、すべての特権操作について、システムの起動及び停止を含めること	9.7.2.1	○		
				9) 監視項目には、すべての特権操作について、入出力装置の取付け・取外しを含めること	9.7.2.1	○		
				10) 監視項目には、認可されていないアクセスの試みについて、失敗したアクセスの試みを含めること	9.7.2.1	○		
				11) 監視項目には、認可されていないアクセスの試みについて、ネットワークのゲートウェイ及びファイアウォールについてのアクセス方針違反及び通知を含めること	9.7.2.1	×		
				12) 監視項目には、認可されていないアクセスの試みについて、侵入検知システムからの警告を含めること	9.7.2.1	×		
				13) 監視項目には、システム警告又は故障について、コンソール警告又はメッセージを含めること	9.7.2.1	○		
				14) 監視項目には、システム警告又は故障について、システム記録例外事項を含めること	9.7.2.1	○		
				15) 監視項目には、システム警告又は故障について、ネットワーク管理警報を含めること	9.7.2.1	○		
			3) 監視の結果は、定期的に見直すこと	1) 監視結果の見直しの頻度は、関係するリスクによって決めること	9.7.2.2	×		
				2) 考慮すべきリスク要因には、業務手続に与える重要性の度合を含める	9.7.2.2	×		
				3) 考慮すべきリスク要因には、関係ある情報の価値、取扱いに慎重を要する度合又は重要性に関する度合を含めること	9.7.2.2	×		
				4) 考慮すべきリスク要因には、システムへの侵入及び誤用の過去の経験を含めること	9.7.2.2	×		
				5) 考慮すべきリスク要因には、システム相互接続の範囲（特に、公衆ネットワーク）を含めること	9.7.2.2	×		
			4) システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること	1) セキュリティのための監視を目的とする重要な事象の識別を補助するために、適切なメッセージタイプを予備の記録として自動的に複製するこ	9.7.2.3	○		
				2) ファイルへ応答指令信号を送る適切なシステムユーティリティ若しくは監査ツールを使用することを考慮す	9.7.2.3	○		
				3) 記録の検証の責任を割り当てるとき、検証する者と活動を監視されている者との間で、役割の分離を考慮	9.7.2.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				4) 記録機能のセキュリティに対して注意すること	9.7.2.3	○		
				5) 管理策は、認可されていない変更及び運用上の問題から保護することを目標とすること	9.7.2.3	○		
			5) コンピュータの時計は正しく設定すること	1) コンピュータ又は通信装置にリアルタイムの時計を作動する機能がある場合、合意された標準時[例えば、万国標準時に（UCT）又は現地の標準時]に合わせること	9.7.3	○		
				2) コンピュータ内の時計は、有意な変化があるかチェックして、あればそれを修正する手順があること	9.7.3	○		
7.8	移動型計算処理及び遠隔作業	移動型計算処理及び遠隔作業の設備を用いるときの情報セキュリティを確実にするため	1) ノート型コンピュータ、パームトップコンピュータ、ラップトップコンピュータ及び携帯電話のような移動型計算処理の設備を用いるとき、業務情報のセキュリティが危険にさらされないような防御を確実にするために、特	1) 移動型計算処理の設備を用いた作業、特に保護されていない環境における作業のリスクを考慮に入れた正式な個別方針を採用すること	9.8.1	×		
				2) 移動型計算処理設備に対する個別方針には、物理的保護、アクセス制御、暗号技術、バックアップ及びウイルス対策についての要求事項などを含めること	9.8.1	×		
				3) 移動型計算処理設備に対する個別方針には、移動型設備をネットワークに接続する場合の規則並びに助言、及び公共の場所で移動型設備を使用する場合の手引も含めること	9.8.1	×		
				4) 公共の場所、会議室、その他組織の敷地外の保護されていない場所で移動型計算処理設備を用いるときは注意を払うこと	9.8.1	×		
				5) 悪意のあるソフトウェアに対抗する手順を整えること	9.8.1	×		
				6) 悪意のあるソフトウェアに対抗する手順は最新のものであること	9.8.1	×		
				7) 移動型計算処理を用いる要員に対する訓練を計画すること	9.8.1	×		
				8) 情報を素早く、容易にバックアップできる装置が利用可能となっていること	9.8.1	×		
				9) これらのバックアップは、情報の盗難、喪失などに対して、十分な保護がなされること	9.8.1	×		
				10) 移動型計算処理設備に含まれる情報の保護は、暗号技術のような管理策を用いて適切に行うこと	9.8.1	×		
				11) ネットワークに接続された移動型設備の使用に対して適切な保護がなされること	9.8.1	×		
				12) 移動型計算処理の設備を用いた、公衆ネットワークを経由して業務情報への遠隔アクセスは、識別及び認証が正しくなされた後でだけ、さらに、適切なアクセス制御機構が備わっているときにだけ、実施されること	9.8.1	×		
				13) 移動型計算処理の設備も、盗難（例えば、車、他の輸送機関、ホテルの部屋、会議室及び集会所に置かれたときの盗難）に対して物理的に保護されること	9.8.1	×		
				14) 大切な、取扱いに慎重を要する及び／又は影響の大きい業務情報が入っている装置は、無人の状態で放置しておかないこと（可能ならば、物理的に施錠するか、又は装置のセキュリティを確保するために特別な錠を用いること）	9.8.1	×		
			2) 遠隔作業を行う場合、組織は、遠隔作業を行う場所に保護を施し、この作業形態のため適切に手	1) 遠隔作業の場所に適切な保護が整っていること	9.8.2	×		
				2) 遠隔作業は、経営陣によって認可され、管理されること	9.8.2	×		
				3) 遠隔作業は、この作業形態のため適切に手配されていること	9.8.2	×		
				4) 組織は、遠隔作業を管理するための個別方針、手順及び標準類を策定することを考慮すること	9.8.2	×		
				5) 組織は、適切なセキュリティの準備及び管理策がなされており、それらが組織のセキュリティ基本方針に適合しているということを十分に確認できた場合にだけ、遠隔作業を認可	9.8.2	×		
				6) 遠隔作業の認可の際には、建物及び周辺環境の物理的セキュリティを考慮に入れた、遠隔作業の場所の既存の物理的なセキュリティを考慮	9.8.2	×		
				7) 遠隔作業の認可の際には、提案された遠隔作業の環境を考慮すること	9.8.2	×		
				8) 遠隔作業の認可の際には、遠隔作業の通信に関するセキュリティ要求事項を考慮すること	9.8.2	×		
				9) 遠隔作業の認可の際には、組織の内部システムへの遠隔アクセスの必要性を考慮すること	9.8.2	×		
				10) 遠隔作業の認可の際には、アクセスされ、通信回線を通過する情報の取扱いに慎重を要する度合を考慮	9.8.2	×		
				11) 遠隔作業の認可の際には、内部システムの取扱いに慎重を要する度合を考慮に入れた要求事項を考慮	9.8.2	×		
				12) 遠隔作業の認可の際には、住環境を共有する者（例えば、家族、友達）からの情報又は資源への認可されていないアクセスの脅威を考慮する	9.8.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				13) 遠隔作業活動のための適切な装置を準備すること	9.8.2	×		
				14) 遠隔作業活動のための適切な保管棚・庫の準備をすること	9.8.2	×		
				15) 遠隔作業活動のための許可される作業を明確にすること	9.8.2	×		
				16) 遠隔作業活動のための作業時間を明確にすること	9.8.2	×		
				17) 遠隔作業活動のための保持してもよい情報の分類を明確にすること	9.8.2	×		
				18) 遠隔作業者のアクセスが認可される内部システム・サービスを明確にすること	9.8.2	×		
				19) 適切な通信装置の準備において、安全な遠隔アクセスを図る方法を明確にすること	9.8.2	×		
				20) 遠隔作業を行う場所の物理的なセキュリティを確保すること	9.8.2	×		
				21) 家族及び来訪者による装置及び情報へのアクセスに関する規則及び手引を明確にすること	9.8.2	×		
				22) ハードウェア及びソフトウェアの支援及び保守の規定を明確にすること	9.8.2	×		
				23) バックアップ及び事業継続のための手順を明確にすること	9.8.2	×		
				24) 監査及びセキュリティの監視を行う	9.8.2	×		
				25) 遠隔作業をやめるときの、監督機関並びにアクセス権限の失効及び装置の返還を明確にすること	9.8.2	×		
8.1	システムのセキュリティ要求事項	情報システムへのセキュリティの組み込みを確実にするため	1) 新しいシステム又は既存のシステムの改善に関する業務上の要求事項には，管理策についての要求事項を明確にするこ	1) セキュリティ要求事項では、システムに組み込まれるべき自動化された制御を考慮すること	10.1.1	×		
				2) セキュリティ要求事項では、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				3) 業務用ソフトウェアのパッケージを評価するときは、システムに組み込まれるべき自動化された制御を考	10.1.1	×		
				4) 業務用ソフトウェアのパッケージを評価するときは、補助対策としての手動による制御の必要性について考慮すること	10.1.1	×		
				5) 適切であれば、管理者は、独立に評価され、認定された製品の利用を考えること	10.1.1	×		
				6) セキュリティ要求事項及び管理策には、関係する情報資産の業務上の価値が反映されること	10.1.1	×		
				7) セキュリティが確保できなかった場合又はセキュリティが確保されていない場合に起こると思われる業務上の損害の可能性もセキュリティ要求事項及び管理策に反映されるこ	10.1.1	×		
8.2	業務用システムのセキュリティ	業務用システムにおける利用者データの消失、変更又は誤用を防止するため	1) 業務用システムに入力されるデータは、正確で適切であることを確実にするために、その妥当性を確認すること	1) 業務取引処理(transaction)、常備データ（名前、住所、信用限度額、顧客参照番号）及びパラメタ（売価、通貨交換レート、税率）の入力を、検査すること	10.2.1	×		
				2) 範囲外の値を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				3) データフィールド中の無効文字を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				4) 入力漏れデータ又は不完全なデータを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				5) データ量の上限及び下限からの超過を検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				6) 認可されていない又は一貫しない制御データを検出するための二重入力又はその他の入力検査を実施すること	10.2.1	×		
				7) 入力データの妥当性及び完全性を確認するために重要なフィールド又はデータファイルの内容の定期的見直しを考慮すること	10.2.1	×		
				8) 入力データに認可されていない変更があるかどうかについての紙に印刷した入力文書の点検を考慮す	10.2.1	×		
				9) 妥当性確認の誤りに対応する手順について考慮すること	10.2.1	×		
				10) 入力データのもっともらしさを試験する手順について考慮すること	10.2.1	×		
				11) データ入力過程に携わっているすべての要員の責任を明確に定めることについて考慮すること	10.2.1	×		
			2) 処理したデータの改変を検出するために，システムに妥当性の検査を組み込むこと	1) 業務用システムの設計は、完全性の喪失につながる誤処理のリスクを最小化するために確実に種々の制限を設けること	10.2.2.1	×		
				2) データ変更を行う追加・削除の機能を持つプログラムの使用及びその位置について考慮すること	10.2.2.1	×		
				3) プログラムが間違った順序で実行されること、又は異常処理の後でプログラムが実行されることを防止する手順について考慮すること	10.2.2.1	×		
				4) データの正しい処理を確実に行うための、異常の状態から回復する正しいプログラムの使用について考慮	10.2.2.1	×		
				5) 取引処理の更新後のデータファイルのバランスをとるための処理又はバッチの制御を考慮すること	10.2.2.1	×		

業務システムのセキュリティに関しては「監視サービス」は保留とする

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				6) 処理開始時のファイル内容を前回終了時のファイル内容と整合を取るための制御を考慮すること	10.2.2.1	×		
				7) システム生成データの妥当性確認を考慮すること	10.2.2.1	×		
				8) 中央コンピュータと遠隔コンピュータとの間で、ダウンロード又はアップロードされたデータ又はソフトウェアの完全性の検査を考慮すること	10.2.2.1	×		
				9) レコード及びファイルの全体のハッシュ合計の検査を考慮すること	10.2.2.1	×		
				10) 業務用プログラムが正しい時刻に確実に実行されることの検査を考慮すること	10.2.2.1	×		
				11) プログラムが正しい順序で実行されることの検査を考慮すること	10.2.2.1	×		
				12) プログラムが正しい順序で実行されない場合は終了され、問題が解決するまでは処理が停止することを確実に実施しているかの検査を考慮	10.2.2.1	×		
			3) 重要性の高いメッセージ内容の完全性を確保するセキュリティ要件が存在する場合に、メッセージ認証の適用を考慮す	1) メッセージ認証の必要性を決定し、最も適切な実施方法を明らかにするために、セキュリティリスクの評価を行うこと	10.2.3	×		
			4) 業務用システムからの出力データについては、保存された情報の処理がシステム環境に対して正しく、適切に行われていることを確実にするために、妥当性確認をするこ	1) 出力データの妥当性確認には、出力データが適当であるかどうかを試験するためのもっともらしさの検査を含むこと	10.2.4	×		
				2) 出力データの妥当性確認には、すべてのデータの処理を確実にするための調整制御の回数を含むこと	10.2.4	×		
				3) 出力データの妥当性確認には、情報の正確さ、完全さ、精度及び分類を明らかにするために、読取り装置又はその後の処理システムにとっての十分な情報の供給を含むこと	10.2.4	×		
				4) 出力データの妥当性確認には、出力の妥当性確認試験に対応する手順を含むこと	10.2.4	×		
				5) 出力データの妥当性確認には、データ出力過程に関わるすべての要員の責任の明確化を含むこと	10.2.4	×		
8.3	暗号による管理策	情報の機密性、真正性又は完全性を保護するため	1) 組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること	1) 暗号技術を用いた解決策が適切であるかどうかに関して決断を下すことは、リスクの評価及び管理策の選択の、広い意味での過程の一部として見ること	10.3.1	×		
				2) 暗号による管理策の使用に関する個別方針を定めるとき、業務情報を保護する上でその基本とする一般原則も含め、組織全体で暗号による管理策を用いることへの管理層を含めた取組みを、考慮すること	10.3.1	×		
			ホスティングに用いるM／Wが暗号化を考慮されている場合△か	3) 暗号による管理策の使用に関する個別方針を定めるとき、かぎを紛失した場合、かぎのセキュリティが脅かされた場合、又はかぎが損傷した場合の暗号化情報を回復させる方法も含め、かぎ管理への取組みを、	10.3.1	×		
			接続サービスのVPNが対象となるか？なる場合△	4) 暗号による管理策の使用に関する個別方針を定めるとき、個別方針の実施の役割及び責任について、考慮すること	10.3.1	×		
				5) 暗号による管理策の使用に関する個別方針を定めるとき、かぎ管理の実施の役割及び責任について、考慮すること	10.3.1	×		
				6) 暗号による管理策の使用に関する個別方針を定めるとき、暗号による適切な保護レベルをどのように決めるかを、考慮すること	10.3.1	×		
				7) 暗号による管理策の使用に関する個別方針を定めるとき、組織全体にわたって効果的に実施するために採用すべき標準類を考慮すること	10.3.1	×		
			2) 取扱いに慎重を要する又は重要な情報の機密性を保護するために，暗号化（Encryption）すること	1) リスクアセスメントに基づき、要求される保護レベルを、使用される暗号アルゴリズムの形式及び品質、並びに使用すべき暗号かぎの長さを考慮して明確にすること	10.3.2	×		
				2) 組織における暗号利用の個別方針を実施するとき、世界の異なる地域における暗号技術の使用、及び国境を越える暗号化情報の流通に関する問題に適用される規制及び国内の制限を考慮すること	10.3.2	×		
				3) 暗号技術の輸出入に適用される規制も考慮すること	10.3.2	×		
				4) 適切な保護レベルを明らかにするため、及び要求される保護レベルを提供し、かぎ管理機能をもつ安全な製品を選択するために、専門家の助言を求めること	10.3.2	×		
				5) 組織が意図した暗号使用に適用される法令及び規制に関して、必要に応じて法律家の助言を求めること	10.3.2	×		
			3) 電子文書の真正性及び完全性を保護するために，ディジタル署名を用いること	1) 秘密かぎの機密性を保護するために注意を払うこと	10.3.3	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 秘密かぎにアクセスした者は、文書に署名でき、その結果かぎの所有者の署名を盗用することがあり得るため、このかぎを秘密に保管するこ	10.3.3	×		
				3) 公開かぎの完全性を保護すること	10.3.3	×		
				4) ディジタル署名に使用される暗号かぎは、暗号化に使用されるものとは異なること	10.3.3	×		
			電子文書の定義 ・業務文書 ・ログを含む監査証跡等 として△とした。	5) ディジタル署名を用いるときは、ディジタル署名がどのような条件のもとで法的拘束力をもつかの条件を規定した関連法令を考慮すること	10.3.3	×		
				6) 電子商取引の場合、ディジタル署名の法的位置付けを知ること	10.3.3	×		
				7) 法的枠組みが不十分である場合、ディジタル署名を使用可能にする拘束力をもつ契約書又は他の合意書を締結すること	10.3.3	×		
				8) 組織によるディジタル署名の使用意図に適用される法律及び規制に関しては、法律家による助言を求める	10.3.3	×		
			4) 事象又は動作が起こったか起こらなかったかについての紛争の解決が必要である場合には，否認防止サービスを用いる	（なし）	10.3.4	×		
			5) 一連の合意された標準類，手順及び方法に基づくかぎ管理システムを，暗号技術の利用を支援するために用いること	1) 共通かぎ暗号技術と公開かぎ暗号技術の二種類の暗号技術を用いることができるように管理システムを運用すること	10.3.5.1	×		
				2) すべてのかぎは、変更及び破壊から保護し、共通かぎ及び秘密かぎは、認可されていない露呈から保護	10.3.5.1	×		
				3) かぎを生成し、保存し、記録保管するために用いられる装置を保護するためには、物理的保護策を用いるこ	10.3.5.1	×		
				4) かぎ管理システムでは、種々の暗号システム及び種々の業務用ソフトウェアのためのかぎを生成する方法を定めること	10.3.5.1	×		
			鍵の必要な暗号 ・データ保存 ・通信暗号（共通鍵） ・ログ保存 とした	5) かぎ管理システムでは、公開かぎ証明書を生成し入手する方法を定めること	10.3.5.1	×		
				6) かぎ管理システムでは、予定している利用者にかぎを配付する方法を定めること	10.3.5.2	×		
				7) かぎ管理システムでは、かぎを保存する方法を定めること	10.3.5.2	×		
				8) かぎ管理システムでは、かぎを変更又は更新する方法を定めること	10.3.5.2	×		
				9) かぎ管理システムでは、セキュリティが損なわれたかぎを処理する方法について定めること	10.3.5.2	×		
				10) かぎ管理システムでは、かぎを無効にする方法について定めること	10.3.5.2	×		
				11) かぎ管理システムでは、事業継続管理の一部として、例えば、暗号化された情報の回復のために、消失したかぎ又は損傷したかぎを回復する方法を定めること	10.3.5.2	×		
				12) かぎ管理システムでは、かぎを、例えば、記録保管された情報又はバックアップされた情報などのために、記録保管する方法について定める	10.3.5.2	×		
				13) かぎ管理システムでは、かぎを破壊する方法を定めること	10.3.5.2	×		
				14) かぎ管理システムでは、かぎ管理に関連する活動を記録し監査する方法を定めること	10.3.5.2	×		
				15) かぎ管理システムでは、セキュリティが損なわれる可能性を軽減するために、かぎは一定期間だけ用いることができるように、かぎの活性化及び非活性化の期日を定めるこ	10.3.5.2	×		
				16) かぎの活性化及び非活性化の期間は、暗号による管理策が使用される環境及び認識されているリスクによって決めること	10.3.5.2	×		
				17) 安全に管理された共通かぎ及び秘密かぎの問題に加え、公開かぎの保護についても考慮すること	10.3.5.2	×		
				18) 公開かぎ証明書を生成する管理手続が信頼できるものであること。例えば、証明機関などの暗号サービスの外部供給者とのサービスレベル契約書又は合意書の内容には、サービス上の義務、信頼性及びサービス提供のための応答時間に	10.3.5.2	×		
8.4	システムファイルのセキュリティ	ITプロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にする	1) 運用システムでのソフトウェアの実行を管理すること	1) 運用プログラムライブラリの更新は、適切な管理者の認可に基づき、任命されたライブラリ管理責任者によってだけ実施されること	10.4.1	○		
				2) 運用システムは、実行可能なコードだけを保持すること	10.4.1	○		
			システムファイルの管理は各サービスを提供する上で必要なものと考えた。	3) 運用システムにおいて、実行可能なコードは、試験の合格及び利用者の受入れの確証が得られ、更に、それに対応するプログラムソースライブラリが更新されるまで、実行しな	10.4.1	○		
				4) 運用プログラムライブラリの更新については、すべて監査記録を維持管理すること	10.4.1	○		
				5) 古い版のソフトウェアは、事故対策用として保持すること	10.4.1	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント）想定対象データ等
						対象	サブコントロール（修正後）	
				6) 運用システムに使用されるベンダー供給ソフトウェアは、供給者によって支援されるレベルで、維持管理され	10.4.1	○		
				7) 新版への更新の決定には、その版のセキュリティ、すなわち、新しいセキュリティ機能の導入又はこの版に影響を及ぼすセキュリティ問題の数及び危険度を考慮すること	10.4.1	○		
				8) セキュリティ上の欠陥を除去するか又は軽減するのに役立つ場合には、ソフトウェアパッチを適用するこ	10.4.1	○		
				9) 供給者による物理的又は論理的アクセスは、支援目的で必要なときに、かつ、管理者の承認を得た場合にだけ、許されること	10.4.1	○		
				10) 供給者の活動は監視されることが望ましい	10.4.1	○		
			2) 試験データを保護し，管理すること 個人情報は業務アプリの範囲即ちホスティングの領域のみと判断した。	1) システム及び受入れの試験は、通常、できるだけ運用データに近い、十分な量の試験データで行うこと	10.4.2	×		
				2) 個人情報が入っている運用データベースは、使用しないようにすること	10.4.2	×		
				3) 個人情報が入っている情報を使用する場合は，使用する前に，個人的要素を消去すること	10.4.2	×		
				4) 試験目的で使用する場合は、運用システムに適用されるアクセス制御手順は、試験用システムにも適用	10.4.2	×		
				5) 試験目的で使用する場合は、運用情報を試験用システムに複製する場合は、その都度、認可を受けるこ	10.4.2	×		
				6) 試験目的で使用する場合は、運用情報は、試験を完了した後直ちに、試験用システムから削除すること	10.4.2	×		
				7) 試験目的で使用する場合は、運用情報の複製及び使用は、監査証跡とするために、記録すること	10.4.2	×		
			3) プログラムソースライブラリへのアクセスに対しては，厳しい管理を維持す 業務ソフトについてはホスティングの領域のみで語ることとした。	1) 可能な限り、プログラムソースライブラリは、運用システムに含めないこと	10.4.3	×		
				2) 各アプリケーションごとに、プログラムライブラリ管理責任者を任命する	10.4.3	×		
				3) IT支援要員に対してプログラムソースライブラリへの無制限のアクセスは与えないこと	10.4.3	×		
				4) 開発又は保守中のプログラムは、運用プログラムソースライブラリに含めないこと	10.4.3	×		
				5) その業務用ソフトウェアのためのIT支援管理者の認可を受けて任命されたライブラリ管理責任者だけが、プログラムソースライブラリの更新及びプログラマへのプログラムソースの発行を実施すること	10.4.3	×		
				6) プログラムリストは、セキュリティの保たれた環境に保持されること	10.4.3	×		
				7) プログラムソースライブラリへのすべてのアクセスについて、監査記録を維持管理すること	10.4.3	×		
				8) ソースプログラムの旧版は、記録保管しておくこと	10.4.3	×		
				9) 旧版のソフトウェアが運用されていた正確な日時を、すべての支援ソフトウェア、ジョブ制御、データ定義及び手順とともに、明確に示すこと	10.4.3	×		
				10) プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従うこと	10.4.3	×		
8.5	開発及び支援過程におけるセキュリティ	業務用システム及び情報のセキュリティを維持するため	1) 情報システムの変更の実施を厳しく管理すること	1) 変更管理手順によって、セキュリティ及び管理手順の完全性が損なわれないこと	10.5.1	×		
				2) 支援プログラマによるシステムへのアクセスはその作業に必要な部分に限定されること	10.5.1	×		
				3) 変更に対する正式な合意及び承認が得られていることを確実にするこ	10.5.1	×		
				4) 業務用ソフトウェア及び運用の変更管理手順は統合されること	10.5.1	×		
				5) 業務用ソフトウェア及び運用の変更過程では、合意された認可レベルの記録の維持を考慮すること	10.5.1	×		
				6) 業務用ソフトウェア及び運用の変更過程では、変更は認可されている利用者によって提出されることを確実にすること	10.5.1	×		
				7) 業務用ソフトウェア及び運用の変更過程では、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするためにこの手順をレビューすること	10.5.1	×		
				8) 業務用ソフトウェア及び運用の変更過程では、修正を必要とするすべてのコンピュータソフトウェア、情報、データベース及びハードウェアを識	10.5.1	×		
				9) 業務用ソフトウェア及び運用の変更過程では、業務用ソフトウェア及び運用の変更作業を開始する前に、提案の詳細について正式な承認を	10.5.1	×		
				10) 業務用ソフトウェア及び運用の変更過程では、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすること	10.5.1	×		
				11) 業務用ソフトウェア及び運用の変更過程では、業務の中断を最小限に抑えるように変更が実行されることを確実にすること	10.5.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				12) 業務用ソフトウェア及び運用の変更過程では、システムに関する一式の文書が各変更の完了時点で更新されること	10.5.1	×		
				13) 業務用ソフトウェア及び運用の変更過程では、古い文書類は記録保管されるか、処分されることを確実に	10.5.1	×		
				14) 業務用ソフトウェア及び運用の変更過程では、すべてのソフトウェアの更新について版数の管理を行うこと	10.5.1	×		
				15) 業務用ソフトウェア及び運用の変更過程では、すべての変更要求の監査証跡を維持管理すること	10.5.1	×		
				16) 業務用ソフトウェア及び運用の変更過程では、運用文書類及び利用者手順は、適切な状態になるように変更されることを確実にすること	10.5.1	×		
				17) 業務用ソフトウェア及び運用の変更過程では、変更の実施は最も適当な時期に行い、関係する業務処理を妨げないことを確実にすること	10.5.1	×		
			2) オペレーティングシステムを変更した場合は，業務用システムをレビューし，試験すること	1) オペレーティングシステムの変更によって業務用ソフトウェアの管理及び完全性に関する手順がそこなわれなかったことを確実にするために、その手順をレビューすること	10.5.2	×		
				2) 年間支援計画及び予算には、オペレーティングシステムの変更の結果として必要となるレビュー及びシステム試験を必ず含めるようにするこ	10.5.2	×		
				3) 実施前に行う適切なレビューに間に合うように、オペレーティングシステムの変更を通知することを確実にす	10.5.2	×		
				4) 事業継続計画に対して適切な変更がなされることを確実にすること	10.5.2	×		
			3) パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更を厳しく管理すること	1) ベンダー供給のパッケージソフトウェアは、変更しないで使用すること	10.5.3	×		
				2) パッケージソフトウェアの変更が絶対必要であると判断された場合は、組み込まれている管理策及び完全性の処理が損なわれるリスクを考	10.5.3	×		
				3) パッケージソフトウェアの変更が絶対必要であると判断された場合は、ベンダーの同意を得るべきかどうかを考慮すること	10.5.3	×		
			業務アプリの実行環境に限った場合。	4) パッケージソフトウェアの変更が絶対必要であると判断された場合は、標準的なプログラム更新として、ベンダーから必要な変更が得られる可能性を考慮すること	10.5.3	×		
				5) パッケージソフトウェアの変更が絶対必要であると判断された場合は、変更の結果として、将来のソフトウェア保守に対して組織が責任を負うようになるかどうかの影響を考慮	10.5.3	×		
				6) 変更が絶対必要と判断された場合、原本のソフトウェアはそのまま保管し、明確に識別された複製に対して変更を行うこと	10.5.3	×		
				7) 変更はすべて、完全に試験すること	10.5.3	×		
				8) 変更はすべて、文書化すること	10.5.3	×		
				9) 将来更新されたソフトウェアに再び適用できるようにすること	10.5.3	×		
			4) 隠れチャネル（Covert channels）及びトロイの木馬（Trojan code）の危険性から保護するために，ソフトウェアの購入，使用及び修正を管理し，検査すること	1) プログラムは定評のある開発元のものだけを購入すること	10.5.4	×		
				2) コードの確認ができるようにソースコードでプログラムを購入すること	10.5.4	×		
				3) 評価された製品を用いること	10.5.4	×		
				4) 使用前にすべてのソースコードを検査すること	10.5.4	×		
				5) 一旦導入したコードへのアクセス及びそのコードへの変更を管理するこ	10.5.4	×		
				6) 重要なシステムでの作業には確実に信頼できる要員を用いること	10.5.4	×		
			5) 外部委託によるソフトウェア開発をセキュリティの保たれたものとするために，管理策を用いるこ	1) ソフトウェア開発を外部委託する場合、使用許諾に関する取決め、コードの所有権及び知的所有権について考慮すること	10.5.5	×		
				2) ソフトウェア開発を外部委託する場合、実施される作業の質及び正確さの認証を考慮すること	10.5.5	×		
				3) ソフトウェア開発を外部委託する場合、外部委託先が不履行の場合の預託（escrow）契約に関する取決めについて考慮すること	10.5.5	×		
				4) ソフトウェア開発を外部委託する場合、なされた作業の質及び正確さの監査のためのアクセス権について考慮すること	10.5.5	×		
				5) ソフトウェア開発を外部委託する場合、コードの品質についての契約要求事項について考慮すること	10.5.5	×		
				6) ソフトウェア開発を外部委託する場合、トロイの木馬を検出するための導入前試験について考慮すること	10.5.5	×		
9.1	事業継続管理の種々の面	事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務手続を保護するため	1) 組織全体を通じて事業継続のための活動を展開し、かつ、維持するための管理された手続が整っていること	1) 重要な業務手続の識別及び優先順位決めも含め、組織が直面しているリスクを、その可能性及び影響の面から理解すること	11.1.1	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				2) 業務手続の中断が事業に及ぼすと思われる影響を理解し（組織の存続性を脅かす可能性のある重大な事件・事故と同様に、より小さめの事故に対処する解決策を見いだすことが重要である）、情報処理施設の事業目的を確立すること	11.1.1	×		
				3) 事業継続の手続の一部をなすこともある適切な保険への加入を考慮	11.1.1	×		
				4) 合意された事業目的及び優先順位に沿って事業継続戦略を明確にし、文書化すること	11.1.1	×		
				5) 合意された戦略に従って事業継続計画を明確にし、文書化すること	11.1.1	×		
				6) 実行されている計画及び手続を定期的に試験し、更新すること	11.1.1	×		
				7) 事業継続管理が組織の手続及び機構に確実に組み込まれるようにする	11.1.1	×		
				8) 事業継続管理手続を調整する責任は、組織内の適切な階層において、例えば、情報セキュリティ委員会において、割り当てること	11.1.1	×		
			2) 事業継続のための活動は、業務手続の中断を引き起こし得る事象を特定することから始めること	1) それらの障害の影響（損害規模及び回復期間の両面から）を判断するために、リスクアセスメントを行うこと	11.1.2	×		
				2) これら両活動の実施には、事業資源及び手続の管理者が全面的に関与すること	11.1.2	×		
			3) 事業継続に対する全般的取組のために、適切なリスクアセスメントに基づいた戦略計画を立てること	1) 事業継続に対する全般的取組方法を決定するための戦略計画は、経営陣の承認を得ること	11.1.2	×		
			4) 重要な業務手続の中断又は障害の後、事業運営を維持又は要求される時間内に復旧させるための計画を立てること	1) 事業継続計画の作成過程では、すべての責任及び緊急時手続を識別し、合意すること	11.1.3	×		
				2) 事業継続計画の作成過程では、要求される時間内に回復及び復旧ができるための緊急時手続を実施す	11.1.3	×		
				3) 事業継続計画の作成過程では、外部事業に対する依存性及び該当する契約事項を評価することに、特に注意すること	11.1.3	×		
				4) 事業継続計画の作成過程では、合意された手順及び過程を文書化す	11.1.3	×		
				5) 事業継続計画の作成過程では、危機管理を含め、合意された緊急時手続及び過程についての、職員の適切な教育を行うこと	11.1.3	×		
				6) 事業継続計画の作成過程では、計画の試験及び更新を行うこと	11.1.3	×		
				7) 計画作成過程は、要求される事業目的、例えば、許容可能な時間内に顧客への特定サービスを復旧することに、重点をおくこと	11.1.3	×		
				8) これを可能にするサービス及び資源を、職員、情報処理施設以外の経営資源、及び情報処理施設の代替手段の手配も含め、考慮すること	11.1.3	×		
			5) すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画の枠組みを維持すること	1) 各事業継続計画では、計画の各要素の実施に対する責任を負う各個人と同様に、その実行開始条件を明確に定めること	11.1.4	×		
				2) 新しい要求事項が明確にされた場合には、確立されている緊急時手続、例えば、避難計画又は既存の代替手段の手配を、適切に修正す	11.1.4	×		
				3) 事業継続計画作成の枠組みでは、各計画を実行に移す前に従うべき手続（状況をどのように評価するか、誰がかかわるべきかなど）を記述した、計画を実施するための条件を考慮すること	11.1.4	×		
				4) 事業継続計画作成の枠組みでは、事業運営及び/又は人命が危険にさらされる事件・事故が発生した場合、取るべき措置について記述した緊急時手続について考慮すること	11.1.4	×		
				5) 緊急時手続には、広報管理についての取決め及び適切な官庁、例えば、警察、消防署及び地方自治体への効果的な連絡についての取決めを含むこと	11.1.4	×		
				6) 事業継続計画作成の枠組みでは、主要な事業活動又は支持サービスの拠点を代替の臨時場所に移動するため、及び業務手続を要求される時間内に回復するために取るべき措置について記述した代替手段の手順について考慮すること	11.1.4	×		
				7) 事業継続計画作成の枠組みでは、正常操業に復帰するために取るべき措置について記述した再開手順について考慮すること	11.1.4	×		
				8) 事業継続計画作成の枠組みでは、計画を何時どのように試験するか、及びその計画を維持するための手続を定めた維持計画予定表について考慮すること	11.1.4	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				9) 事業継続計画作成の枠組みでは、事業継続手続を理解させ、手続が継続して有効であることを確保するために計画される認識及び教育活動について考慮すること	11.1.4	×		
				10) 事業継続計画作成の枠組みでは、個人の責任について考慮すること	11.1.4	×		
				11) 事業継続計画作成の枠組みでは、計画のどの構成要素を実行するのに誰が責任をもつかを記述すること	11.1.4	×		
				12) 事業継続計画作成の枠組みでは、必要に応じて、構成要素を実行する、代わりの責任者を任命すること	11.1.4	×		
				13) 事業継続計画作成の枠組みでは、各計画には特定の責任者がいるこ	11.1.4	×		
				14) 緊急時手続、手動による代替手段の手配、及び再開計画は、該当する事業資源又は関連する手続きの管理者の責任範囲内でたてること	11.1.4	×		
				15) 情報処理及び通信施設のような代替技術サービスにおける代替手段の手配は、通常、サービス供給者の責任とすること	11.1.4	×		
			6) 事業継続計画が最新の情報を取り入れた効果的なものであることを確実にするために、定期的に試験すること	1) 事業継続計画の試験は、また、回復チームのすべてのメンバー及び他の関連職員がそれらの計画を確実に認識するものであること	11.1.5.1	×		
				2) 事業継続計画の試験スケジュールでは、計画の各要素をどのようにして、何時試験すべきかを示すこと	11.1.5.1	×		
				3) 計画の個々の構成要素を、頻繁に試験すること	11.1.5.1	×		
				4) 計画が実際に役立つことを保証するために、様々な手法を使用するこ	11.1.5.1	×		
				5) 様々な状況の机上試験を行うこと（障害例を用いての事業回復計画の検討）	11.1.5.1	×		
				6) 模擬試験を行うこと（特に、事件・事故後又は危機管理における役割についての要員の訓練）	11.1.5.1	×		
				7) 技術的回復試験を行うこと（情報システムを有効に復旧できることを確実にする）	11.1.5.1	×		
				8) 代替施設における回復試験を行うこと（主構内から離れた場所で回復運転と並行して業務手続を実施す	11.1.5.1	×		
				9) 供給者施設及びサービスの試験を行うこと（外部からの供給によるサービス及び製品が契約事項を満たすことを確認する）	11.1.5.1	×		
				10) 全体的な模擬回復試験を行うこと（組織、スタッフ、装置、施設及び手続が障害に対処できることを試験す	11.1.5.1	×		
				11) いずれの組織もこれらの手法を使用することができるが、これらの手法には個別の回復計画の特質を反映させること	11.1.5.1	×		
			7) 事業継続計画は、それらの有効性を継続して確保するために、定期的な見直し及び更新によって維持すること	1) 事業継続上の問題を適切に対処することを確実にするための手順は、組織の変更管理プログラムの中に含まれること	11.1.5.2	×		
				2) 各事業継続計画の定期的見直しに対する責任を割り当てること	11.1.5.2	×		
				3) 事業継続計画にいまだ反映されていない事業計画の変更を識別し、それに続いて事業継続計画を適切に更新すること	11.1.5.2	×		
				4) この正式な変更管理手続は、更新された計画を配付し、計画全体の定期的見直しによって強化することを確実にするものであること	11.1.5.2	×		
10.1	法的要求事項への適合	刑法及び民法、その他の法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避ける	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること	1) 各情報システムについて、すべての関連する法令、規制及び契約上の要求事項に適合する特定の管理策、及び個々の責任も同様に明確に定め、文書化すること	12.1.1	×		
			2) 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は，法的制限事項に適合するように，適切な手続を実行す	1) ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること	12.1.2.2	×		
				2) ソフトウェア製品の取得手続に関する標準類を発行すること	12.1.2.2	×		
				3) ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること	12.1.2.2	×		
				4) 適切な財産登録簿を維持管理すること	12.1.2.2	×		
				5) 使用許諾書、マスターディスク、手引などの所有権の証拠書類及び証拠物件を維持管理すること	12.1.2.2	×		
				6) 許容された利用者の最大数を超過しないことを確実にするための管理策を実行すること	12.1.2.2	×		
				7) 認可されているソフトウェア及び使用許諾されている製品だけが導入されていることを確認すること	12.1.2.2	×		
				8) 適切な使用許諾条件を維持管理するための個別方針を定めること	12.1.2.2	×		
				9) ソフトウェアの処分又は他人への譲渡についての個別方針を定めること	12.1.2.2	×		
				10) 適切な監査ツールを用いること	12.1.2.2	×		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				11) 公衆ネットワークから入手するソフトウェア及び情報の使用条件に従うこ	12.1.2.2	×		
			3) 組織の重要な記録は、消失、破壊及び改ざんから保護されること	1) 記録類は、記録の種類（例えば、会計記録、データベース記録、業務処理記録、監査及び記録、運用手順）及びそれぞれの種類について保持期間及び記録媒体の種類（例えば、紙、マイクロフィッシュ、磁気媒体、光学媒体）の詳細も定めておく	12.1.3	×		
				2) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎを、安全に保管すること	12.1.3	×		
				3) 暗号化されたアーカイブ又はディジタル署名にかかわる暗号かぎは、必要なときに、認可されている者が使用できるようにすること	12.1.3	×		
				4) 記録の保管に用いられる媒体が劣化する可能性を考慮すること	12.1.3	×		
				5) 保管及び取扱いの手順は、製造業者の推奨に従って実行すること	12.1.3	×		
				6) 電子記録媒体が用いられるところでは、将来の技術変化によって読むことが出来なくなることから保護するために、保持期間を通じてデータにアクセスできること（媒体及び書式の読取り可能性）を確保する手順を	12.1.3	×		
				7) 要求されるすべての記録を、受け入れられる時間内に、受け入れられる書式で取り出すことができるように、データ保管システムを選択すること	12.1.3	×		
				8) 保管及び取扱いシステムは、記録及びそれらの法令上又は規制上の保持期間の明確な識別を確実にす	12.1.3	×		
				9) 保持期間が終了した後、組織にとって必要ないならば、そのシステムは、記録を適切に破棄できること	12.1.3	×		
				10) 記録及び情報の保持、保管、取扱い及び処分に関する指針を発行す	12.1.3	×		
				11) 重要な記録の種類及びそれらの記録の保持期間を明確にした保持計画を作成すること	12.1.3	×		
				12) 主要な情報の出典一覧を維持管理すること	12.1.3	×		
				13) 重要な記録及び情報を消失、破壊及び改ざんから保護するための適切な管理策を実行すること	12.1.3	○ 認証（入退）ロ		
			4) 関連する法令に従って個人情報を保護するために，管理策を用いること	1) データ保護の担当責任者を任命すること	12.1.4	×		
				2) 個人情報を構造化されたファイルに保管しようという提案のいかなるものについてもデータ保護の担当責任者に報告することは、データ所有者の責任であること	12.1.4	×		
				3) 関連法規法令に定められるデータ保護の原則に対する意識を確実にすることも、データ所有者の責任で	12.1.4	×		
			5) 情報処理施設の使用には管理者の認可を要するものとし，そのような施設の誤用を防ぐための管理策を用いること	1) 業務以外の目的又は認可されていない目的のために、管理者の承認なしにこれらの施設を使用することは、施設の不適切な使用と見なされること	12.1.5	×		
				2) 施設の不適切な使用が、監視又は他の手段で明らかにされた場合、関係する個々の管理者に通知し、適切な懲戒措置を取ること	12.1.5	×		
				3) 情報処理施設の誤用の防止のための監視手続を実行する前に、法的な助言を受けること	12.1.5	×		
				4) すべての利用者は、その許可されたアクセスの正確な範囲を認識していること	12.1.5	×		
				5) 組織の従業員及び外部利用者には、認可されている場合を除き、アクセスは許可されないということを通知すること	12.1.5	×		
				6) ログオン時に、アクセスしようとしているシステムが、秘密のものであり、認可されていないアクセスは許可されない旨を知らせる警告メッセージをコンピュータの画面上に表	12.1.5	×		
				7) 利用者は、引き続きログオン処理を行うために画面上のメッセージに同意し、それに適切に対応すること	12.1.5	×		
			6) 暗号による管理策の策定においては、国の法律への適合を確実なものにするために，法的な助言を求めること	1) 暗号化された情報又は暗号管理策を他国にもち出す前にも、法的な助言を受けること	12.1.6	×		
			7) 人又は組織に対する措置を支援するには，十分な証拠をもつこと	1) 人又は組織に対する措置が内部の懲戒問題にかかわるものであるならば、必要な証拠は、内部手続によって示されること	12.1.7.1	×		
				2) 紙文書の場合、原本を安全に保管し、誰がそれを発見し、どこでそれを発見し、何時それを発見し、誰がその発見に立ち会ったかの記録をとる	12.1.7.1	×		
				3) 紙文書の場合、どのような調査をおこなっても、原本に手が加えられないことが、証明できること	12.1.7.3	×		
				4) コンピュータ媒体上の情報の場合、取外し可能な媒体、ハードディスク又は記憶装置内の情報はすべて、可用性を確保するために複製をとっ	12.1.7.3	○		

項番	項目	目的	コントロール	サブコントロール	JIS X 5080 :2002	ファシリティ関連		備考（コメント） 想定対象データ等
						対象	サブコントロール（修正後）	
				5) コンピュータ媒体上の情報の場合、コピー処理中のすべての行為について記録を保存し、その処理には、立会い者が居ること	12.1.7.3	×		
				6) コンピュータ媒体上の情報の場合、媒体の複製一組及びその記録を、安全に保管すること	12.1.7.3	×		
				7) 法的な措置が予想される場合は、早めに弁護士又は警察に相談し、必要な証拠についての助言を得る	12.1.7.3	×		
10.2	セキュリティ基本方針及び技術適合のレビュー	組織のセキュリティ基本方針及び標準類へのシステムの適合を確実にするため	1) 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること	1) 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的な見直しを考慮すること	12.2.1	×		
				2) 情報システムの所有者は、その所有するシステムが適切なセキュリティの基本方針、標準類、その他のセキュリティ要求事項に適合しているかどうかに関して、定期的に見直しが行われることを支持すること	12.2.1	×		
			2) 情報システムは，セキュリティ実行標準と適合していることを定期的に検査すること	1) 技術適合の検査としては、ハードウェア及びソフトウェアの管理策が正しく実行されていることを確実にするため、運用システムの検査を行	12.2.2	○		
				2) 技術適合の検査では、専門家の技術援助を得ること	12.2.2	×		
				3) 技術適合の検査は、経験をもつシステムエンジニアが手動で（必要ならば、適切なソフトウェアツールによる支援を得て）行うか、又は、技術専門家による解釈の結果として技術報告書を作成する自動パッケージソフトウェアによって実施されるこ	12.2.2	○		
				4) 侵入試験の成功によりシステムのセキュリティが損なわれたり、他のぜい（脆）弱性を不注意に悪用される可能性に注意すること	12.2.2	×		
				5) いかなる技術適合チェックも、資格をもち認可されている者によって、又はその監督のもとでのみ、実施さ	12.2.2	×		
10.3	システム監査の考慮事項	システム監査手続の有効性を最大限にすること、及びシステム監査手続への/からの干渉を最小限にするため	1) 監査要求事項、及び、運用システムの検査を含む監査活動は、業務手続の中断のリスクを最小限に抑えるように、慎重に計画を立て、合意され	1) 監査要求事項は、担当経営陣の同意を得ること	12.3.1	×		
				2) 検査の範囲は、合意され、管理されること	12.3.1	×		
				3) 検査は、ソフトウェア及びデータへの読出し専用アクセスに限定するこ	12.3.1	×		
				4) 読出し専用以外のアクセスは、システムファイルから隔離された複製に対してだけ許可されること	12.3.1	×		
				5) 複製ファイルは、監査が完了した時点で消去すること	12.3.1	×		
				6) 検査を実施するための情報資源は、明確に識別され、利用可能であ	12.3.1	×		
				7) 特別又は追加処理の要求事項は、識別され、合意されること	12.3.1	×		
				8) すべてのアクセスは、照合用の証跡を残すために、監視され、記録さ	12.3.1	×		
				9) すべての手順、要求事項及び責任について、文書化すること	12.3.1	×		
			2) システム監査ツール、すなわち、ソフトウェア又はデータファイルへのアクセスは、誤用又は悪用を防止するために、保護されること	1) システム監査ツールは、開発及び運用システムから分離しておくこと	12.3.2	×		
				2) システム監査ツールは、テープライブラリ、又は利用者の領域で保持しないこと	12.3.2	×		

第１編　第３部　技術部会ＷＧ３

リスクアセスメント手法についての検討報告書

平成 17 年 3 月 31 日

第１編　第３部　目次

１．序章 176
　１．１　本報告書の目的 176
　１．２　アプローチ 177
２．事例モデル 180
　２．１　設定 180
　２．２　企業のプロファイル 180
　２．３　業務フロー 182
　２．４　製品開発情報に関する業務フロー 183
　２．５　J 社のネットワーク構成 185
　２．６　各フロアや拠点の見取り図 186
３．進捗状況と今後 188
　３．１　モデルについて 188
　３．２　リスクアセスメント手法の選択 188
　３．３　今後の予定と課題 188
４．添付資料 189
　４．１　資産台帳案 190
　４．２　GMITS におけるリスク基準レベル案 194
　４．３　GMITS における部分的なリスクアセスメント結果案 195

技術部会ＷＧ３ 参加及び報告書作成メンバーリスト（敬称略）

（ＷＧ３リーダ）

株式会社アズジェント	駒瀬　彰彦

（ＷＧ３メンバー：氏名５０音順）

株式会社日立製作所	相羽　律子
株式会社ディアイティ	池田　秀司
株式会社ソルクシーズ	内山　和子
株式会社情報数理研究所	閑野　忠和
株式会社富士通ソーシアルサイエンスラボラトリ	高野　晃太朗
株式会社ジェイエムシー	宮崎　亮

１．序章

情報セキュリティ監査制度は、我が国の情報セキュリティ全体の向上に貢献するとともに、情報セキュリティを達成、維持することを目的としている。

本リスクアセスメント手法についての検討報告書（以下、「本報告書」という。）は、情報セキュリティ監査制度において、被監査主体が適切にリスクアセスメントを実施する、監査主体が被監査主体において実施したリスクアセスメント手法や内容の妥当性を判断する、また、契約時に被監査主体の業務内容などから監査項目や作業工数の割出しのために自らリスクアセスメントを行うなど、監査主体、被監査主体の双方のために作成された。

従って、本調査報告書本の主な読者は、情報セキュリティマネジメントシステムの構築を検討もしくは着手している被監査主体において、実際に情報セキュリティマネジメントシステムの構築に携っている方及びその責任者、特にリスクアセスメント及びその結果に基づくリスク対応を行う責任者、監査主体においては、監査計画を立案する、作業工数を見積る、監査内容を決定する情報セキュリティ監査員の方を想定している。

本報告書の作成にあたり、ご協力頂いた情報セキュリティ監査協会の Tech-WG3 委員会の委員の皆様をはじめご協力頂いた関係各位に対し厚く御礼申し上げる。

１．１　本報告書の目的

昨今の様々なセキュリティ事件、事故が各種のメディアで報道されている。このような脅威に対する対応に際して、技術的なシステム対策だけでは不十分であり、情報セキュリティを網羅的に向上させるためには、情報資産（情報及びそれを取り扱う人、システム、施設など）を的確に把握し、どのようなリスクを保有しているのかを分析し、必要に応じて適切な対応をとり、変動するリスクに対して定期的な監視による見直しをかけ、適時改善するというリスクマネジメントのフレームワークが不可欠となる。　本報告書では、リスクアセスメントプロセスに有用な手法及びその特徴などについての理解を深めるために想定リスクアセスメント対象となる仮想モデルを設置し、実際にいくつかのリスクアセスメント手法を適用し、各々の手法に基づくプロセス、すなわち、リスクアセスメントに必要な情報収集から分析、そこから導かれる結果等の比較検討を行い、どのような場面において、どのリスクアセスメント手法が有用であるかを判定することを目的とした検討項目についての報告を試みる。

リスクアセスメント手法は、その手法から導かれる結果から、定性的、定量的に大別されることがある。理想的には汎用的で適切に定量的なリスク値を与える手法が望まれるが、統計データ不足や分析に要する作業工数などから、このような手法の確立は困難な面を多く抱えている。また、昨今の IT を中心とした社会インフラの構造においては、技術革新も早く、それに伴い脅威も増加している。このようなめまぐるしく変化する環境に対しても、十分対応できるリスクアセスメント手法の確立も期待されている。本報告書では、数種類のリスクアセスメント手法を紹介し、どのような局面でどのような手法が効果的であるの

か、などの判定を行う過程において検討されている項目について報告するものである。

１．２　アプローチ

本目的を達成するために採用しているアプローチについての概要を説明する。

１．２．１　モデル事例アプローチ

まず、リスクアセスメント手法を比較検討するにあたり、想定リスクアセスメント対象となる仮想モデルを設置する必要があると考えた。このモデルにおいては、全体的に仮想モデルの業務内容、人員構成、ネットワーク構成、施設などが大まかにわかる範囲に留め、リスクアセスメント手法を適用する際、必要となる情報については、各々のリスクアセスメント手法を適用する過程で、どのような情報をどのような方法で入手する必要があるのかなどを検討することにした。このことで、仮想モデルが汎用的に利用できることを期待している。

次章において、このモデルを照会する。

１．２．２　リスクアセスメント手法の検討

次に、どのような手法を適用するかについての検討が行われた。候補としては、前年度の報告書に紹介した表１に示されるものが対象となった。

表1　情報セキュリティのリスクアセスメント手法

用途　A:経営面のリスク評価に効果的　B:資産のリスク評価に効果的　C:特定分野に効果的

No.	手法	手法の特徴	用途
1	GMITS（Guidelines for the Management for IT Security）	ISO/IEC TR13335が紹介しているITセキュリティの分析手法である。情報資産の価値と関連する脅威の大きさとぜい弱性の大きさからリスク値を算定する。	A B
2	DISC PD3002（BS7799－GAP方式）	GMITSの情報資産の範囲をITから一般の情報資産にまで拡大したアプローチを取る。予め採用を決めたセキュリティのガイドラインをベースにし、脅威とぜい弱性を分析することにより、組織のコントロールの実施状況を評価するGAP分析手法である。	B
3	JRAM（JIPDEC Risk Analysis Method）	ホスト集中型システムを対象にした質問票の回答結果からぜい弱性を洗い出して点検評価し、JRAM分析シートで、過去のセキュリティ事故の損失額を洗い出す。システムの安全性が合格レベルにあるか計ることを目的としている。	A
4	JRMS	企業全体のリスクマネジメントがベース。JRAMを改良	A

	（JRAM 2002）	してネットワーク分散型システム向きにした質問票で、得点方式、定性的リスク分析、定量的事故解析による、ぜい弱性を分析するリスク分析方法である。	
5	CRAMM（CCTA Risk Analysis and Management Methodology）	英国大蔵省（CCTA）と英国規格協会（BSI）が共同開発した。資産の識別、資産評価を質的技法と量的技法を併用している。脅威、ぜい弱性を定量化し、推奨する対策を生成し、リスクを許容レベルにする。	B
6	ALE（Annual Loss Exposure）	米国商務省標準局NISTが事象の損害額と発生確率から年間予想損失額を近似計算で算定する。各情報資産のALEをCIA別に分類集計する。	B
7	FTA（Fault Tree Analysis）	システムの信頼性･安全上、望まない事象全て想定し、原因事象を階層的に表現する。故障、不正動作、人的エラー等の因果関係を示し、発生確率から事故発生確率が出る。最近では情報セキュリティにおいても詳細で厳密な対策を取るものに適用できる。	B C

また、この表のリスト以外のリスクアセスメント手法として、2004年にIPA（独立行政法人 情報処理推進機構）に報告されたリスクアセスメント手法（（以下、「IPA方式」という。））（http://www.ipa.go.jp/security/fy15/development/metrics/index.html）の適用についても検討している。

１．２．３　リスクアセスメント手法の選択と評価

（１）定量的/定性的評価の観点

リスクアセスメントには、リスクを金額などの数値により示すもの、相対的な数値で示すもの、定性的な評価を示すものがある。

金額換算により評価する定量的手法は、そこから導かれた結果に対して判断がしやすく経営者にとって理解しやすい方法である。定量的手法は、リスク対策に必要なコストと対策効果を判断するために、リスクを損失予測額や他の数値基準に基づいて把握した予測式などを使い、将来や現在と異なる場合のリスクの予測を分析する。

一方、個々のリスク要因を詳細に分析評価するまえに、全体のバランスからリスクの概要を把握することが優先される場合がある。ある場面においては、数値基準によるよりも本来すでに適用し運用していなければならない管理策と現状との乖離を識別することによる定性的な分析による対策で充分なものもある。例えば、「強行法規」※への順守に対するリスクの評価などはこれにあたると考えられる。

この、定量的・定性的評価の観点に立ち、モデルに対し、各々のリスクアセスメン

ト手法を適用することで、どの場面においては、どのリスクアセスメントアプローチが有用であるかの判断材料と成りえると考える。

※「強行法規」

強行法規とはその規定が適用される人の意思によってその内容を左右することが許されない規定をいう。例えば刑法の殺人罪の規定は、人の意思によって内容を左右することは許されないため強行法規である。また、安全対策を求める個人情報保護法２０条は、個人情報取扱事業者が安全対策を行うか否かについての意思の自由を許さない強行法規である。

（2） 経営的な観点からのアプローチと技術的な観点からのアプアプローチ

経営方針や戦略上の観点からセキュリティ要求事項を明確にしてリスクを把握する経営・管理的アプローチ（以下マネジィアルアプローチ：Managial Approach という。）と、技術要因をベースにして、予測される現象や原因からリスクを把握するアプローチ（以下テクニカルアプローチ：Technical approach という。）がある。

例えば金融業界等では経営的観点から、全体のリスクの把握が優先されるが、それぞれ個々のリスク要因は、具体的な管理的・金額的に把握され、経営者が判断できるものでなければならない。

一方、原子力産業や航空宇宙産業および社会的に使われる大規模な電子情報通信システムなどでは、技術面からのリスク分析が最も優先されなければならないものである。情報リスク分析手法でも、経営的観点からのマネジィアルアプローチにより情報資産を特定し、それについて特定のテクニカルアプローチを選択してリスク対策を決定し、それ以外は一般のリスク分析によるアプローチを選択し、それらの結果を組み合わせる手法はリスクアセスメントのコスト･パフォーマンスの面から検討に値するものである。

今回の検討においては、マネジィアルアプローチにおける視点からの考察をモデルに適用することは困難と考え、テクニカルアプローチにおける視点に立ち、各々のリスクアセスメント手法の有効性について判定するものと考える。

２．事例モデル

各々のリスクアセスメント手法の特性や有効性を判断するために､仮想企業を設定する。ここでは中堅の製造販売業を営む「株式会社 JASA」（以降 J 社という。）を設定し、実際にその組織の情報資産に対するリスクアセスメントを実施することをねらいとする。

２．１　設定

J 社は PC の各種部品や周辺機器の製造販売をしている中堅企業である。古くから半導体の開発メーカとしてコンピュータの各種部品の開発を行い国内の主要メーカに OEM 提供していたが、自ら PC の周辺機器を組み立て、自社ブランドで一般消費者や企業ユーザに販売することも行っている。大容量携帯型記憶装置のブームの影響もあり、J 社が自社開発した「J-USB トークン」が一般の消費者に好評で J 社の主力製品になりつつある。「J-USB トークン」は大容量のデータの蓄積のみならず暗号化の機能も備えたものである。このような機能の開発のノウハウも半導体開発の実績によって培われてきたものである。従来は製品カタログを作成し、主要な顧客に DM を配信したり、雑誌や新聞の広告欄に商品を掲載して商品を販売したりしていた。近年はインターネットショッピングサイトでの運用を開始し、インターネットショッピングサイトでの売上げも着実に伸びてきている。

２．２　企業のプロファイル

J 社の組織構成として、社長及び取締役で構成される取締役会を経営方針の決定機関とし、総務部、営業本部、製品開発部、製造部の事業部門によって構成される。取締役は 5 名いるが、内３名は営業本部、製品開発部、製造部の部長を兼務している。

社長直属の部門として広報企画室が設置され、製品カタログの作成や雑誌や新聞での広告の掲載、自社 WEB サーバからの情報配信等のマーケティング活動を行っている。

総務部は人事課と総務課で構成され､経理や人事､スタッフの勤怠管理､社内設備管理､各種社内文書の管理等を主な業務としている。

営業本部は流通事業部、E コマース事業部、大阪営業所、技術部で構成される。流通事業部では従来の製品カタログや雑誌及び新聞広告を媒体とした営業活動を行っている。また、同業他社と比較しても遜色のない開発力を持っている背景から、現在でも国内の主要メーカに対するコンピュータ周辺機器の各種部品を OEM 提供するといった営業活動も行っている。E コマース事業部はインターネットショッピングサイト運用が開始された時に設立された部門である。インターネットショッピングサイトに関連する顧客対応が主な業務となっている。インターネットショッピングサイトのメンテナンスも技術部に協力を得ながら実質的な管理を行っている｡技術部は社内ネットワーク及びサーバのメンテナンス、自社ブランドの商品のマニュアル作成、製品の技術サポート、営業支援、製品設置支援等

が主な業務となっている。大阪営業所は関西方面の営業拠点となっており、流通事業部及び技術部の機能を持ち、独自に営業展開を行っている。

製品開発部は製品のハードウエア的な仕様に関する開発やドライバやアプリケーションに関する開発を主な業務としている。

製造部 PC の周辺機器を自社ブランドとして販売を開始した時期に設立された部門である。主に PC の周辺機器の大量受注に対する製造業務、自社ブランドの周辺機器の組み立て業務が主な業務である。

表 2-1　J 社の組織構成

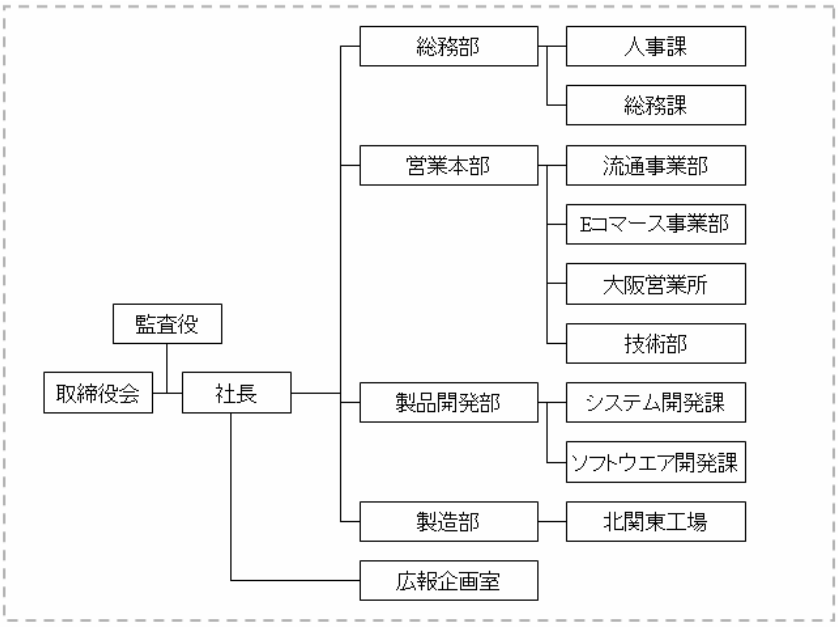


表 2-2-1　企業プロファイル

企業規模	
売上高	約 50 億円　（利益 10%）
従業員	約 80 名
従業員の人数	
総務部	約 5 名
流通事業部	約 15 名
E コマース事業部	約 10 名
大阪営業所	約 5 名
技術部	約 15 名
システム開発課	約 5 名
ソフトウエア開発課	約 5 名
製造部（北関東工場）	約 25 名

広報企画室	3 名

表 2-2-2　売れ筋の製品と売上げに占める割合

J-USB トークン	外付 USB 対応大容量記憶装置 （OS 対応ドライバ付属、簡易暗号化ソフトウエア付属）	20%
J-SuperDisk	ATA ハードウエア RAID システム （ハードディスクユーティリティソフトウエア付属、フラッシュメモリ型 OS 搭載）	15%
JASA Simple UPS	UPS （管理ソフトウエア付属、フラッシュメモリ型 OS 搭載）	10%
J-RAID	PCI バス接続 ATA RAID カード （OS 対応ドライバ付属）	10%
JASA Secret BackUP	マルチ OS 対応暗号化ネットワークドライブ環境構築ソフトウエア	10%

表 2-2-3　保有する顧客情報

顧客情報	顧客情報の内訳	保有件数
DM 配信用顧客リスト	企業ユーザ（70%）、個人ユーザ（30%）	3,000 件
インターネット会員	企業ユーザ（10%）、個人ユーザ（90%）	5,000 件
保守ユーザ	企業ユーザ（50%）、個人ユーザ（50%）	20,000 件
受発注記録（1 年間保存）	企業ユーザ（50%）、個人ユーザ（50%）	150,000 件

２．３　業務フロー

J 社は高度な開発力を背景として成長している会社である。そのため従来から開発情報の管理を厳格に行ってきた。社長はもともと製品開発に携わってきた主要メンバーの一人であり、社長就任時から研究開発や技術情報を守ることの重要性を社内に徹底してきた。今や経営者としての業務が中心となったが、この努力が他社との差別化を実現し会社が発展していった要因のひとつであると自負している。

ところが、ある日社長が残業を終えて最終退室時の確認を行っている際に営業社員のゴミ箱から製品開発に関する機密情報を含んだ資料が捨ててあるのを偶然発見した。最近頻繁に報道される各社の情報漏洩に関して危機感をいただいていた社長は、翌日各部門の責任者を緊急で招集し会議を行った。会議では営業本部長が後日 J 社の製品開発情報に関する業務フロー及びネットワーク構成を、総務部長は各フロアや拠点の見取り図を提出することとなった。

２．４　製品開発情報に関する業務フロー

製品開発情報に関する業務フローを整理すると、大きく分けて 2 通りのフローが存在することが確認された。一つは製品開発部から流通事業部を経由して顧客に至るフローである（表 2-3-1)。国内の主要メーカに対してコンピュータの周辺機器の各種部品やアプリケーションを OEM 提供する際の営業活動として最低限の製品仕様の説明を顧客にする必要がある。その場合文書や媒体によって情報が直接顧客に伝わることはない。開発担当者は製品ごとに存在する開発情報提供に関するガイドラインに従い口頭にて営業担当者に対して必要な情報を提供している。営業担当者はその情報を基に開発情報を顧客に対して口頭もしくはプレゼン資料として紙の媒体で顧客に提供している。案件が具体的になると営業担当者は開発担当者に営業同行を依頼する場合もある。その場合は、営業担当者立会いのもと口頭にて開発情報の提供が顧客に対して行われる。ただし、開発担当者が単独で顧客を訪問することはない。

国内の主要メーカと OEM 契約が成立した際には、社内において機密とされている製品の開発情報が一定の手順に従って顧客に提供される。営業担当者は顧客との技術提供に関する契約を担当する。契約内容は毎週定期的に開催される経営会議で承認されることになっている。営業担当者は社内で承認され、双方で合意された契約書及び「開発情報提供に関する依頼書」を総務部の情報管理担当者に提出する。情報管理担当者は情報管理規定に従い「開発情報提供に関する依頼書」の承認を行い、情報の管理番号を発行し管理する。情報管理規定には、顧客に対して開発情報を提供する場合、紙の文書もしくは媒体で提供を行う旨が記されている。

もう一つは製品開発部から製造部に至るフローがある（表 2-3-2)。製造部の担当者は製品毎に決められており、情報は製品開発部のネットワークからその製品に関する情報を共有することができる。また、必要であれば電話や打ち合わせ等で直接開発担当者から口頭で情報提供を受ける場合もある。社内規定で印刷やデータのコピーは禁じられているため、製造部の端末や事務所には開発情報は残らないことになっている。また、製造部の製造担当者は会社と厳密な機密保持契約を締結している。

表 2-3-1　製品開発情報に関する業務フロー（製品開発部～流通事業部～顧客）

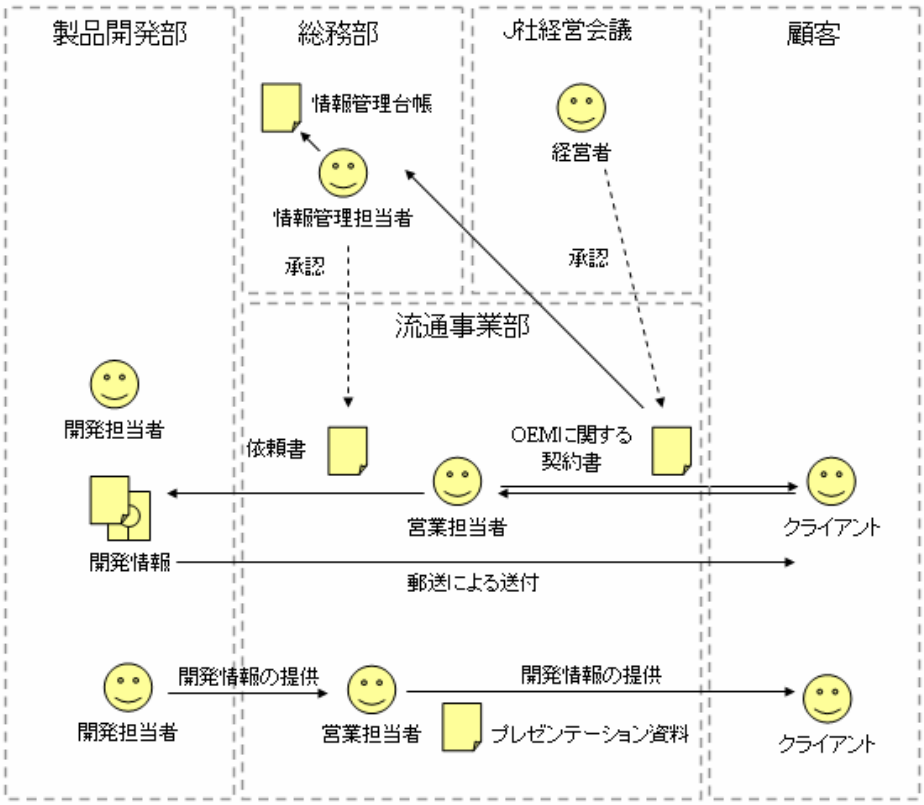


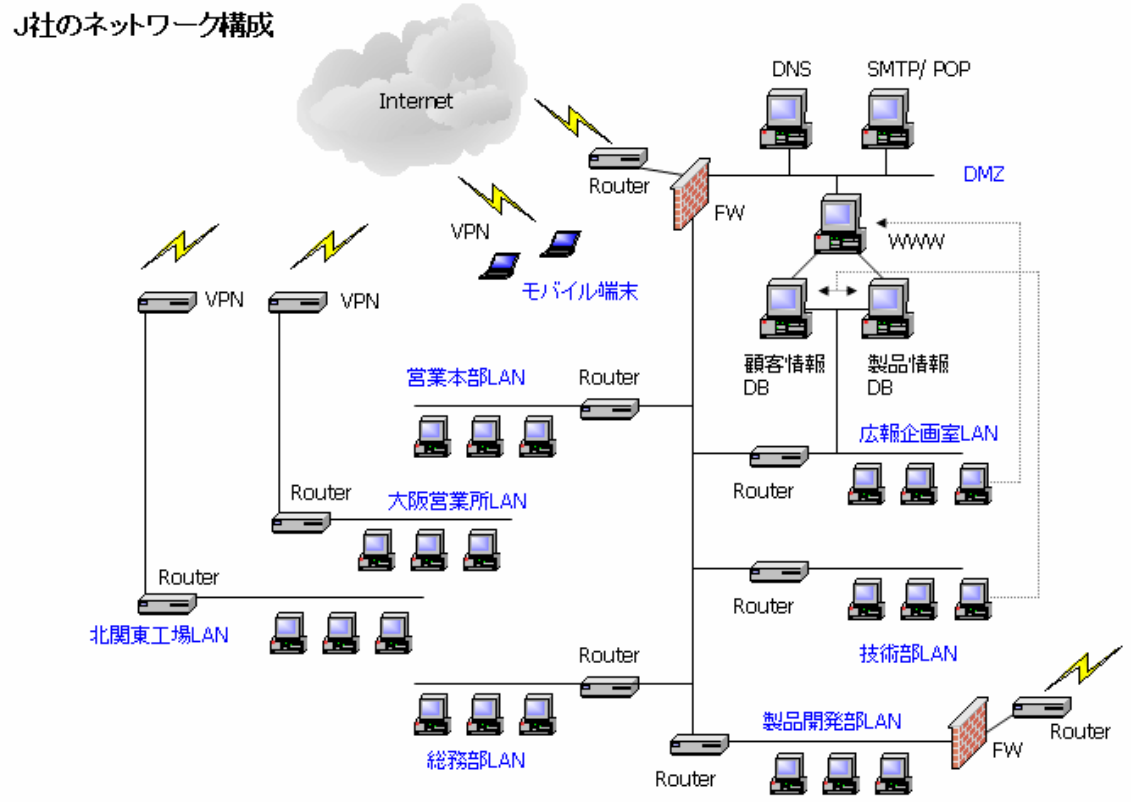
表 2-3-2　製品開発情報に関する業務フロー（製品開発部～製造部）

２．５　Ｊ社のネットワーク構成

各拠点間はインターネットで接続されており、VPN ゲートウエイをそれぞれの拠点に設置している。インターネット回線は上位プロバイダーと契約をしており、ネットワークや各種サーバの管理は全て自社で行っている。本社は一般業務用と開発用途としての回線を契約しており、業務用途の回線は技術部が、開発用途の回線は開発部が管理運用している。それぞれの部署毎にネットワークがセグメントで分割されアクセス制御がされている。

営業担当者はモバイルでの接続が許可されており、外出先から指定された端末を用いて VPN 接続を行っている。

表 2-4　J 社のネットワーク構成



２．６　各フロアや拠点の見取り図

J 社の拠点は国内に 3 箇所ある。東京の丸の内に東京本社があり、20 階建てのビルの 17 階と 18 階の一部を賃貸している。それぞれの区画に対してはアクセス制御がされており、非接触型のカードを持った許可された人しか入室ができないようなセキュリティが施されている。

大阪の淀屋橋には、大阪営業所があり、10 階建てのビルの 7 階を賃貸している。サーバルームには物理的な施錠を施してあり、一般社員や外部の者がアクセスできないようになっている。受付の区域に人が入ると音楽が流れるようになっており、通常、訪問者は受付より内線で事務所に連絡をする。ただし宅配業者は顔見知りであるため、そのまま受付を通り過ぎて荷物を集荷している。月に数回は営業時間でも担当者が不在になるときがあるので、その時はオフィースを施錠して留守電付のインターフォンで対応している。

群馬県内には、北関東工場があり、2 階建ての自社工場となっている。作業場では製品の組み立てや生産が行われており、ロビー横に位置する事務所の守衛担当者の横を通らないと中には入室ができないようになっている。ロビー横の事務所を通る際には必ず社員証を提示することになっている。事務所は 2 階にもあり、作業場を経由しないと行けないようになっている。サーバルームは物理的に施錠がされており、許可された者しか入室ができないようになっている。

表 2-5-1　各フロアや拠点の見取り図　本社

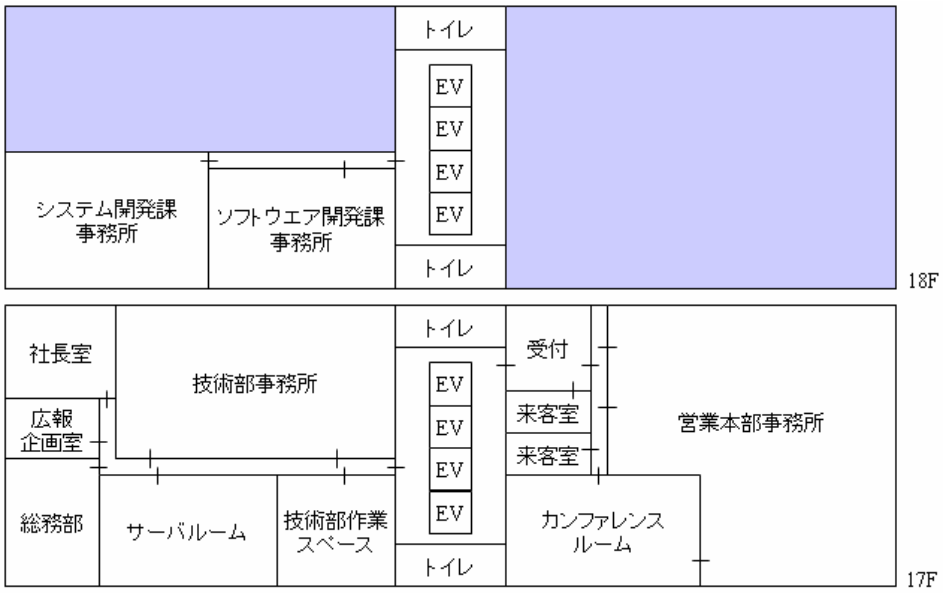


表 2-5-2　各フロアや拠点の見取り図　大阪営業所

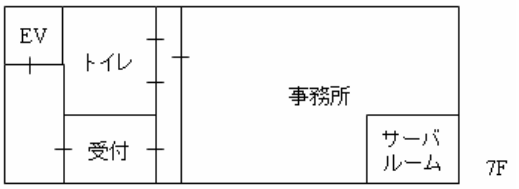
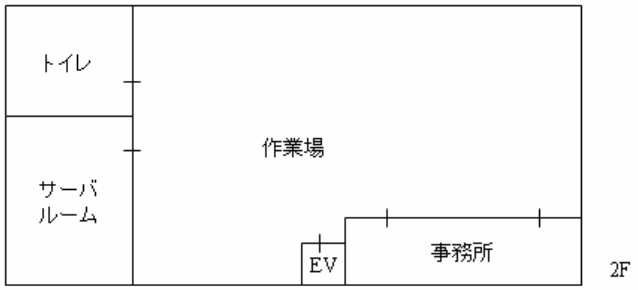
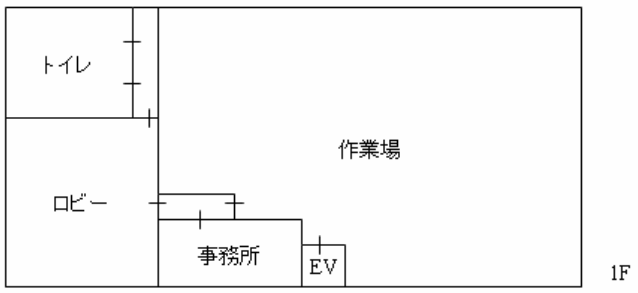


表 2-5-3　各フロアや拠点の見取り図　北関東工場





３．進捗状況と今後

現在、当初の目的を達成すべく作業を進めているところであり、ここまでの進捗状況について報告する。

３．１　モデルについて

リスクアセスメント手法の評価を行うために利用する 2 章で紹介したモデルについては、概ね完成した。各々のリスクアセスメント手法を適用する上でモデル上に必要な追加情報等があれば、今後リスクアセスメントを行う過程で、それらのプロセス内で紹介される予定である。

３．２　リスクアセスメント手法の選択

現在、GMITS、IPA方式、FTAによるリスクアセスメントについて検討をしている。
GMITSに関しては、本WG内で分析に必要となる情報資産の洗い出し、リスク評価が部分的に検討されている。(付録資料参照)
FTAに関しては、本モデルを想定した際、リスク分析の対象範囲が広いことから、すべてのケースにおいてFTAの利用は現実的でないという意見もあるため、実現したとしても部分的な範囲の評価に終わる可能性がある。
IPA方式は、セキュリティ対策の程度を定量的に把握しようとする手法である。これは、これまでのセキュリティ評価手法の多くが、着眼点を列挙し「実施しているか、否か」を二者択一で答えていくいわゆるチェックリストに対し、メトリクス（指標）を明確にした上で数値化しようとする手法である。この考え方は今日の複雑化したセキュリティプロセスにおいては、適合するメトリクスがうまく提示できれば、極めて有効な手法と成り得る。しかしながら、それを推進していく為には、基礎データの蓄積が欠かせないが、現在のところはその収集の目処は立っていないため、現在どのようそのメトリクスを作成し、モデルに適用するかを検討中である。

３．３　今後の予定と課題

目的達成のための作業を継続して行う。具体的には、

1）適用するリスクアセスメント手法の決定と実施
2）リスクアセスメント結果の評価
3）リスクアセスメント手法の評価
4）リスクアセスメントプロセスにおいて、検討された脅威･ぜい弱性の一覧作成
5）監査主体、被監査主体が各々のリスクアセスメント手法を適用する際の留意点の洗い出し　等

である。

４．添付資料

現段階では、WG内では、コンセンサスを得ておらず、未承認ではあるが、各作業において検討されている項目について報告する。
対象となっている手法はGMITSによるものである。

4章の構成

章番号	タイトル
4.1	資産台帳案　(1)、(2)、(3)
4.2	GMITSにおけるリスク基準レベル案
4.3	GMITSにおける部分的なリスクアセスメント結果案

※　注意

構成中、4.1（3)、4.2、4.3　（表中は青文字を利用）は、一連の作業結果であり、互いに関連性（依存性）があるが、4.1（1）および４．１（2）は、それらとは独立しており、且つ各々も独立している。従って、４．１．(1）及び４．１（2）は、独立したファーマットの案としてのみ有用であると思われる。

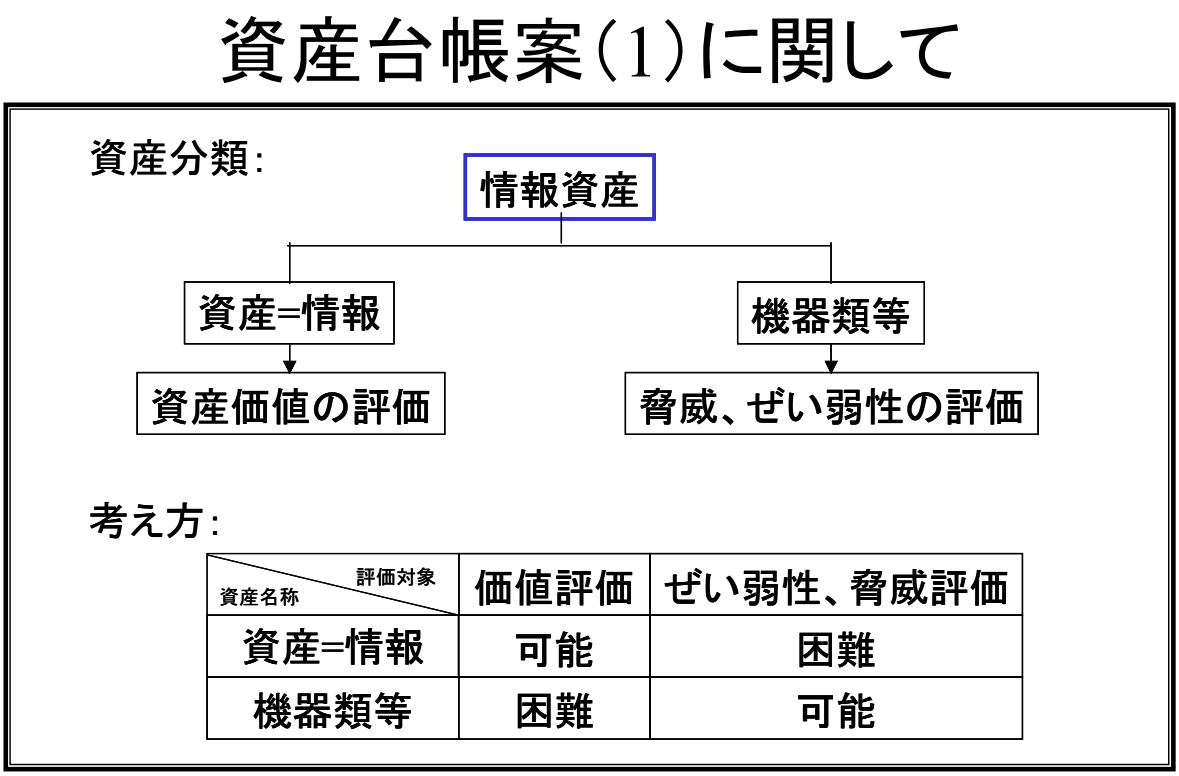
４．１　資産台帳案

資産台帳案（１）　（４．２、　４．３とは独立）

資産台帳案（1）について概要を説明する。

ここでの、基本的な考え方は、情報資産を「資産（=情報)」と「機器類等」として分類し、「機器類等」を「資産」の入れ物ととらえ、「資産」に属する「保管場所」欄に「機器類等」を挿入し、紐付けをする方式である。この方式は、「資産（=情報)」は可能、「ぜい弱性・脅威」評価は困難、他方、「機器類等」は、価値評価は困難、「ぜい弱性・脅威」評価は可能という考えに基づいている（図4-1参照）。

図4-1　資産台帳案（1）の考え方



この考え方を、モデル事例に適用し、作業をしたものを次の表（表4-1）にまとめる。現時点では、網羅性などの点で十分ではない。

表4-1　情報資産台帳案（1）

		次ステップの評価に必要と思われる要素				
	資産名	詳細	保管場所	変化形		作業者コメント
資産						
1	製品	PCの各種部品、周辺機器	工場の作業場			
2	製品開発情報	・製品仕様情報 ・開発情報 ↑のレベルで資産名にあげる必要があるかもしれない、また、その他があるかもしれない	HW04	2a	製品カタログ	2a～2fのレベルで資産名としてあげる必要があるか？ 変化形へのデータの流れや変化系それぞれの ・形態（電子or紙） ・保管場所 を明らかにする必要があるのかもしれない
				2b	DM	
				2c	インターネットショッピングサイト用の情報	
				2d	WEBで配信する情報	
				2e	雑誌・新聞広告用の情報	
				2f	商品のマニュアル	
3	顧客情報		HW03			表2-3の項目に細分化して資産名にあげる必要があるか？
4	OEMに関する契約書		本社（事務所－流通事業部）			
5	開発情報提供に関する依頼書		本社（事務所－流通事業部）			
6	情報管理台帳		本社（事務所－総務部）			
7	機密保持契約書		本社（事務所－？部）			
機器類等						
HW01	WWWサーバ	1台？	本社（サーバルーム）			
HW02	クライアントPC（社内作業用）	？台	本社（事務所） 大阪営業所（事務所） 北関東工場（事務所）			
HW03	モバイルPC	？台	－			
HW04	顧客情報DB専用PC	1台？	本社（サーバルーム？）			
HW05	製品情報DB専用PC	1台？	本社（サーバルーム？）			
HW06	Router	5台	本社（事務所）			
HW07	Router（外部と接続用1）	2台	本社（サーバルーム）			
HW08	Router（外部と接続用2）	2台	大阪営業所（サーバルーム？） 北関東工場（事務所）			
HW09	FW	2台	本社（サーバルーム）			

表中、「資産（=情報）」には、数字の資産IDを「機器類等」には、HWから始まる資産IDを付与している。また、「資産」の欄にある「保管場所」は、「機器類等」で付与されたIDを追記していく予定である。

資産台帳案（2）（４．２、　４．３とは独立）

情報資産台帳

様式番号：IS-006
Ver.1.0

大分類	小分類	内容	保管場所		保管期間	管理者	資産価値		
			紙	データ			機密性	完全性	可用性
製品開発	USBトークン製品開発情報	J-USBトークン開発情報、仕様書	製品開発部共有キャビネット	製品開発部共有サーバ	無期限	開発部門長	3	3	3
	RAIDシステム製品開発情報	J-SuperDiskトークン開発情報、仕様書	製品開発部共有キャビネット	製品開発部共有サーバ	無期限	開発部門長	3	3	3
	UPSシステム製品開発情報	JASA Simple UPSトークン開発情報、仕様	製品開発部共有キャビネット	製品開発部共有サーバ	無期限	開発部門長	3	3	3
	RAIDカード製品開発情報	J-RAID開発情報、仕様書	製品開発部共有キャビネット	製品開発部共有サーバ	無期限	開発部門長	3	3	3
	暗号化ソフト製品開発情報	JASA Secret BackUP開発情報、仕様書	製品開発部共有キャビネット	製品開発部共有サーバ	無期限	開発部門長	3	3	3
顧客個人情報	DM配信用顧客リスト	氏名、住所、電話番号、FAX番号	営業本部共有キャビネット	営業本部共有サーバ	無期限	営業部門長	3	3	3
	インターネット会員	氏名、住所、電話番号、メールアドレス	営業本部共有キャビネット	営業本部共有サーバ	無期限	営業部門長	3	3	3
	保守ユーザ	企業名、氏名、住所、電話番号、メールアドレス	営業本部共有キャビネット	営業本部共有サーバ	無期限	営業部門長	3	3	3
	受発注記録	受発注記録	営業本部共有キャビネット	営業本部共有サーバ	1年間	営業部門長	3	3	3
顧客企業情報	納入先システム構成表、構成図	システム構成、原価計算書、システムイメージ、レイアウト	技術部共有キャビネット	技術部共有サーバ	納品後、1年	技術部門長	3	3	3
	導入関連ファイル	現在進行中の導入物件の仕様書構成な	技術部共有キャビネット	技術部共有サーバ	納品後、1年	技術部門長	3	1	1
	過去の導入物件ファイル	過去の導入物件の仕様書構成	技術部共有キャビネット	営業本部共有サーバ	納品後、1年	営業部門長	2	1	1
	顧客資料	住所他／営業情報入札仕様書等	技術部共有キャビネット	営業本部共有サーバ	納品後、1年	営業部門長	2	1	1
	契約書	OEM契約、保守契約、売買契約	営業本部共有キャビネット	営業本部共有サーバ	無期限	営業部門長	2	1	1
営業情報	見積データ・見積控え	客先提出見積書及び原価書	営業本部共有キャビネット	営業本部共有サーバ	7年	営業部門長	2	1	1
	提案書	入札／コンペ用提案資料	営業本部共有キャビネット	営業本部共有サーバ	7年	営業部門長	2	2	2
	価格・仕切表	営業見積用資料	営業本部共有キャビネット	営業本部共有サーバ	―	営業部門長	2	3	1
	見積・受注・売上他管理	社内データ	営業本部共有キャビネット	営業本部共有サーバ	無期限	営業部門長	2	3	1
	顧客マップ	担当者名簿 納入先と導入時期	営業本部共有キャビネット	営業本部共有サーバ	無期限	営業部門長	3	3	1
	営業セミナー参加者リスト	営業セミナー参加者リストおよびアン	営業本部共有キャビネット	営業本部共有サーバ	2年	営業部門長	3	2	1
従業員個人情報	雇用社員個人情報	社員個人情報	人事部門キャビネット	人事部門共有サーバ	無期限	人事部門長	3	3	2
	応募者個人情報	面接・選考 履歴書・職歴書	人事部門キャビネット	人事部門共有サーバ	新卒者については2年保管で廃棄	人事部門長	3	3	2
	賃金	給与・賞与・退職金	人事部門キャビネット	人事部門共有サーバ	無期限	人事部門長	3	3	1
	社会保険	健康・厚生年金・厚生年金基金・労災・雇用保険等	人事部門キャビネット	人事部門共有サーバ	無期限	人事部門長	3	3	1

資産台帳案（3)（４．２、　４．３と関連）

番号	資産	オーナー	形式	種別	備考	資産価値					
						漏洩	理由	改ざん	理由	喪失	理由
101	開発情報	製品開発部	ｻｰﾊﾞ	文書		3		3		3	
102	ﾌﾟﾚｾﾞﾝﾃｰｼｮﾝ資料	流通事業部	ｻｰﾊﾞ	記録		3		2		1	作れば良い
103	ﾌﾟﾚｾﾞﾝﾃｰｼｮﾝ資料	流通事業部	印刷物	記録	本資料、またはその作成途中のものが、ｺﾞﾐ箱から発見された機密情報を含む資料と考えられる	3		2		1	印刷すれば良い
104	OEM契約書	流通事業部	ｻｰﾊﾞ	記録		2		2		1	作れば良い
105	OEM契約書	流通事業部	印刷物	記録		2		2		2	
106	仕様書	製品開発部	ｻｰﾊﾞ	文書		3		3		3	
107	仕様書	製品開発部	媒体	文書		3		3		1	作成すれば良い
108	仕様書	製品開発部	印刷物	文書		3		3		1	印刷すれば良い
109	仕様書	流通事業部	媒体	文書		3		3		1	作成すれば良い
110	仕様書	流通事業部	印刷物	文書		3		3		1	印刷すれば良い
201	製品情報	製品開発部	ｻｰﾊﾞ	文書		3		3		3	
202	製品情報	製造部	ｻｰﾊﾞ	文書	製品開発部ｻｰﾊﾞ閲覧のみならなし	3		3		3	
301	インターネットショッピングサービ	Eコマース事業部	–	ｻｰﾋﾞｽ		3		3		3	
401	顧客情報	Eコマース事業部	ｻｰﾊﾞ	個人情報		2		2		2	

４．２　GMITS におけるリスク基準レベル案

リスク基準レベル案（３）

資産価値

レベル	資産価値	備考
1	10万円	100万円未満
2	1000万円	100万円以上、1億円未満
3	10億円	1億円以上

脆弱性

レベル	脆弱性	備考
1	対策の効果でリスクが1/10000に低減	対策によるリスクの低減が1/1000以上
2	対策の効果でリスクが1/100に低減	対策によるリスクの低減が1/10以上、1/1000未満
3	対策の効果がない	対策によるリスクの低減が1/10未満

脅威の発生頻度

レベル	脅威の発生頻度	備考
1	事件・事故が起きる可能性は低い	事件・事故の予想発生頻度は100年に1回未満
2	事件・事故が起きる可能性がある	事件・事故の予想発生頻度は年1回未満、100年に1回以上
3	いつ事件・事故が起きても不思議ではない	事件・事故の予想発生頻度は年1回以上

リスク

レベル	リスク	備考
1	年0.01円	年0.1円未満
2	年1円	年0.1円以上、10円未満
3	年100円	年10円以上、1000円未満
4	年1万円	年1000円以上、10万円未満
5	年100万円	年10万円以上、1000万円未満
6	年1億円	年1000万円以上、10億円未満
7	年100億円	年10億円以上

４．３　GMITS における部分的なリスクアセスメント結果案

リスクアセスメント結果案（３）

脆弱性					資産	脅威		リスク
ISMS Ver.2.0			備考	脆弱性レベル	資産価値レベル	脅威	脅威の発生頻度レベ	リスクレベル
資産103								
8.(6)②	媒体の処分	媒体が不要となった場合は、安全、かつ、確実に処分すること。		2	3	ｺﾞﾐ箱に捨てられた機密情報を含んだ資料から、競合企業に機密情報が漏洩し、優位性を喪失した。	2	5
資産301								
8.(7)⑥	公開されているｼｽﾃﾑ	情報を公開する前に正式な認可の手続きがとられ、また、情報の改ざんを防止するために公開した情報の完全性を保護すること。		2	3	ミスにより1/100の価格を設定。	3	6
10.(2)①	入力ﾃﾞｰﾀの妥当性確認	業務用ｼｽﾃﾑに入力されるﾃﾞｰﾀは、正確で適切であることを確実にするために、その妥当性を確認すること。		2	3	販売価格のシステム的なチェックがなくミスによる1/100で販売(しかも販売数量を無制限に…)	3	6
資産401								
9.(2)③	利用者のﾊﾟｽﾜｰﾄﾞの管理	ﾊﾟｽﾜｰﾄﾞの割当ては、正規の管理手順によって統制すること。	共通アカウントを利用しているが、異動があってもアカウント、パスワードの変更をしていない	3	2	退職者から犯罪者へアカウントとパスワードが漏洩。 その結果顧客の個人情報が漏洩。	3	6